UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

Robin Forslund, Timothy Kelly, George Lenz, Jr., Matthew Menting, Donalyn North, Robin Rector, Eric Ottenheimer, Gail Rossi, and Gregory Williams, *on behalf of themselves and all others similarly situated*, Plaintiffs, v. R. R. Donnelley & Sons Company, Defendant.	Case No. 1:22-cv-04260 JUDGE JOHN J. THARP, JR **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Robin Forslund, Timothy Kelly, George Lenz, Jr., Matthew Menting, Donalyn North, Robin Rector, Eric Ottenheimer, Gail Rossi, and Gregory Williams ("Plaintiffs") bring this Consolidated Class Action Complaint against R.R. Donnelley & Sons Company ("RRD" or "Defendant"), individually and on 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:

NATURE OF THE ACTION

1. Conti is a well-known ransomware group that has attacked more than 400 organizations worldwide (including more than 290 in the United States) over the span of more than a year. It generally uses the same *modus operandi*, hacking and exfiltrating sensitive data of an organization and then holding it for ransom. The FBI and others have issued warnings and advisories—advisories that provide detailed instructions for how to avoid a Conti attack. Widely available software has been developed that protects against Conti attacks.

2. RRD, a Fortune 500 marketing, packaging and printing company with a global client base and more than 32,000 employees, did not protect itself from this known threat. In fact, it not only failed to meet regulatory and industry standards for cybersecurity, but also failed to take the most basic security measures such as encryption of data and destruction of obsolete data. As a result, on or around November 29, 2021, RRD experienced unauthorized access to its network containing the highly sensitive personal information of its current and former employees' (the "Data Breach").

3. The personally identifiable information ("PII") accessed and exfiltrated in the Data Breach included its employees' names, addresses, Social Security numbers, dates of birth, and driver's license numbers. There are reports that after the Data Breach, Conti leaked 2.5 gigabytes of this PII to the internet.[1]

4. RRD's cybersecurity and monitoring practices were so poor that it failed to detect the unauthorized intrusion into its systems for approximately one month. Defendant then waited approximately eight months before it started mailing notification letters to victims. These notices abhorrently downplayed the severity of the Data Breach by omitting, *inter alia*, that 2.5 gigabytes of data had already been leaked to the internet.

5. During the course of its business operations, Defendant obtained, collected, utilized, and derived a benefit from Plaintiffs' and Class Members' PII; therefore, RRD owed and otherwise assumed statutory, regulatory, contractual, and common law duties and obligations, including to keep Plaintiffs' and Class Members' PII confidential, safe, secure, and protected from the type of unauthorized access, disclosure, and theft that occurred in the Data Breach.

[1] https://www.bleepingcomputer.com/news/security/marketing-giant-rrd-confirms-data-theft-in-conti-ransomware-attack/ (last visited Oct. 14, 2022).

6. In providing and entrusting their PII to Defendant through the course of their employment with Defendant, Plaintiffs and those similarly situated relied upon and reasonably expected Defendant to maintain and protect the security and privacy of their PII and to comply with its duties and obligations.

7. Defendant expressly and impliedly understood its obligations and promised to safeguard Plaintiffs' and Class Members' PII. But for this mutual understanding, Plaintiffs and Class Members would not have provided Defendant with their PII. Defendant, however, did not meet these reasonable expectations, causing Plaintiffs and Class Members to suffer injury.

8. While many details of the Data Breach remain in the exclusive control of Defendant, upon information and belief, Defendant breached its duties and obligations by failing, in one or more of the following ways: (1) failing to design, implement and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train employees on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiffs and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the PII; (7) failing to recognize or detect that Conti had accessed its network in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent Conti ransomware, and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

9. As a result of Defendant's acts and omissions, Plaintiffs and Class Members had their most sensitive PII stolen by malicious cybercriminals. The information that was compromised is, in essence, one-stop shopping for identity thieves to wreak complete financial havoc on

Plaintiffs' and Class Members' lives. Given the sensitivity and static nature of the information involved (such as names, Social Security numbers, dates of birth and driver's license numbers), the risk of identity theft is present, materialized and will continue into the foreseeable future for Plaintiffs and the Class Members. Plaintiffs and Class Members will therefore now live with the present and ongoing risk of identity theft, which will require third-party professional services to monitor their PII for criminal misuse and dark web activity.

10. As a direct result of the Data Breach, Plaintiffs and Class Members have suffered the following actual and imminent injuries: (i) invasion of privacy, (ii) out-of-pocket expenses, (iii) loss-of time and productivity incurred mitigating the present risk and imminent threat of identity theft, (iv) actual identity theft and fraud resulting in additional economic and non-economic damages; (v) diminution of value of their PII; (vi) anxiety, stress, nuisance, and annoyance; (vii) increased targeted and fraudulent robocalls and phishing email attempts; (viii) the present and continuing risk of identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (ix) the retention of the reasonable value of the PII entrusted to Defendant; and (x) the present and continued risk to PII, which remains on Defendant's vulnerable network, placing Plaintiffs and Class Members at an ongoing risk of harm.

11. Plaintiffs seek to remedy these harms, on behalf of themselves and all similarly situated persons whose PII was compromised in the Data Breach. Plaintiffs seek compensatory damages, incidental damages, and consequential damages for the invasion of privacy, loss of time, loss of productivity, out-of-pocket costs, and future costs of necessary identity theft monitoring. Plaintiffs also seek injunctive relief including improvements to Defendant's data security system and protocols, deletion of PII that is unnecessary for legitimate business purposes, and future annual audits to protect their PII against foreseeable future cyber security incidents.

12. Plaintiffs bring this Class Action Complaint against Defendant seeking redress for its unlawful conduct, asserting claims for: (1) negligence, (2) breach of implied contract, (3) unjust enrichment, (4) invasion of privacy, (5) violations of the Illinois Consumer Fraud and Deceptive Business Practices Act ("CFA"), (6) violations of the New York Labor Law, and (7) declaratory judgment/injunctive relief.

PARTIES

13. Plaintiff Robin Forslund is a natural person and citizen of Michigan residing in Flint, Michigan, where he intends to remain.

14. Plaintiff Timothy Kelly is a natural person and citizen of Tennessee residing in Attoka, Tennessee, where he intends to remain.

15. Plaintiff George Lenz is a natural person and citizen of New York residing in Niagara Falls, New York, where he intends to remain.

16. Plaintiff Matthew Menting is a natural person and citizen of Wisconsin residing in Green Bay, Wisconsin, where they intend to remain.

17. Plaintiff Donalyn North is a natural person and citizen of Oregon residing in Forest Grove, Oregon, where she intends to remain.

18. Plaintiff Eric Ottenheimer is a natural person and citizen of Nevada residing in Carson City, Nevada, where he intends to remain.

19. Plaintiff Robin Rector is a natural person and citizen of Indiana residing in Ladoga, Indiana, where she intends to remain.

20. Plaintiff Gail Rossi is a natural person and citizen of Arizona residing in Scottsdale, Arizona, where she intends to remain.

21. Plaintiff Gregory Williams is a natural person and citizen of New Jersey residing in Branchburg, New Jersey, where he intends to remain.

22. Defendant R.R. Donnelley & Sons Company is a corporation organized under the laws of Delaware, and its United States headquarters and principal place of business is located at 35 W. Wacker, 36th Floor, Chicago, IL 60601.

JURISDICTION AND VENUE

23. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

24. The Northern District of Illinois has personal jurisdiction over Defendant named in this action because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conducts substantial business in Illinois and this District through its headquarters, offices, parents, and affiliates.

25. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

Defendant's Business and Promises

26. RRD describes itself as an integrated multichannel marketing communications service company that has been in business for over 150 years. According to its website, RRD has more than 32,000 employees and has 176 business locations worldwide.

27. RRD collects a wide range of PII and other sensitive data as part of its regular business. Upon information and belief, RRD maintains:

a. Basic personal details, such as names, addresses, contact details, dates of birth, age, gender, and marital status;

b. Unique identifiers such as National Insurance Number or pension scheme reference number;

c. Demographic details, such as information about age, gender, race, marital status, lifestyle, and insurance requirements;

d. Employment information such as role, employment status (such as full/part time, contract), salary information, employment benefits, and employment history;

e. Health information such as information about your health status, medical records and medical assessment outcomes;

f. Benefits information such as benefit elections, pension entitlement information, date of retirement and any relevant matters impacting your benefits such as voluntary contributions, pension sharing orders, tax protections or other adjustments;

g. Financial details such as payment card and bank account details, details of credit history and bankruptcy status, salary, tax code, third-party deductions, bonus payments, benefits and entitlement data, national insurance contributions details;

h. Claims details such as information about any claims concerning employer's insurance policy;

i. Marketing preferences;

j. Online information: e.g., information about visits to its websites;

k. Events information such as information about interest in and attendance at our events, including provision of feedback forms;

l. Social media information such as interactions (e.g., likes and posts); and

m. Criminal records information such as the existence of or alleged criminal offences, or confirmation of clean criminal records.

28. Plaintiffs and Class Members directly or indirectly entrusted Defendant with sensitive and confidential information, including their PII, which includes information that is static, does not change, and can be used to commit myriad financial crimes. Plaintiffs and Class Members relied on the sophistication of Defendant's business to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII.

29. Plaintiffs and Class Members directly or indirectly entrusted their PII to Defendant on the condition of their employment. Said differently, if Plaintiffs and Class Members had not provided their PII to Defendant, they would have been unable to work for Defendant. Plaintiffs understood when they provided their PII to Defendant that it would be securely maintained and, if they had known Defendant would not do so, Plaintiffs would not have provided it with their PII.

30. Employees place value in data privacy and security. These are important considerations when deciding who to work and provide services for. Plaintiffs would not have applied for or accepted employment with Defendant, nor provided their PII, had they known that RRD does not take all reasonable precautions to secure the personal and financial data given to it by its employees.

31. Defendant's Privacy Policy ("Privacy Policy") implicitly recognizes the risk and foreseeability of cybersecurity incidents and also recognizes that RRD has a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties.

32. Defendant's Privacy Policy applies to any personal information provided to RRD and any personal information that RRD collects from other source." RRD's Privacy Policy also represents:

> The security of your personal data is important to us. We follow generally accepted industry standards to protect the personal data submitted to us, both during transmission and once we receive it.
>
> RRD uses reasonable measures to safeguard personally identifiable data, which measures are appropriate to the type of data maintained and follows applicable laws regarding safeguarding any such data under our control. In addition, in some areas of our Sites, RRD may use encryption technology to enhance data privacy and help prevent loss, misuse, or alteration of the data under RRD's control. RRD also employs industry-standard measures and processes for detecting and responding to inappropriate attempts to breach our systems.[2]

33. Regarding the deletion of personal information Defendant no longer needs, the Privacy Policy represents as follows:

> Depending on the country in which you live, work or access our Site(s), your data may be retained for a reasonable time for use in future contact with you, or for future improvements to RRD services. In the event the data you provide to us is an application for employment, that application will be held in accordance with our HR records management policy.[3]

The Data Breach

34. On or about August 5, 2022, Defendant began sending notices to victims of the Data Breach (the "Notice of Data Breach"). Defendant also notified various state Attorneys

[2] https://www.rrd.com/privacy-policy
[3] *Id.*

General of the Data Breach and provided the Attorneys General with "sample" notices of the Data Breach. In an August 5, 2022 letter to the Washington Attorney General, Defendant :

> On December 23, 2021, RRD identified a systems intrusion in its technical environment. The Company promptly implemented a series of containment measures to address this situation, including activating its incident response protocols, shutting down its servers and systems and commencing a forensic investigation. Based on observed tactics, RRD identified the Threat Actor as being affiliated with a foreign ransomware group. RRD also determined that the Threat Actor gained access through a phishing attack that targeted several employees on or about November 29, 2021. RRD notified and is working with appropriate law enforcement authorities. Following this incident, RRD has also enriched its monitoring and analysis capabilities to combat future cyber threats.
>
> RRD initially did not believe that the Threat Actor had removed any data from its environment. However, in mid-January 2022, RRD became aware that certain of its corporate data was accessed and exfiltrated by the Threat Actor. It evaluated the affected data with the assistance of a third-party data discovery provider and ultimately identified certain employee personal data among the documents exfiltrated. RRD also determined that the exfiltrated documents included certain data related to clients for whom RRD provides printing and mailing services. It has notified the affected clients accordingly. It expended significant effort to review each of the documents in order to identify potentially affected clients and individuals…. Affected documents included names, addresses, social security numbers, and, in some cases, dates of birth, and/or driver's license numbers….[4]

35. In addition to the above letter, the notification letters received by Plaintiffs similarly confirm that PII exposed in the Data Breach includes names, addresses, Social Security numbers, dates of birth, and driver's license numbers.

36. Defendant has publicly admitted that the unauthorized actors accessed and exfiltrated files containing Plaintiffs' and Class Members' PII. However, Defendant has failed to provide sufficient information to Plaintiffs and Class Members that would allow them to appreciate

[4] For example, an August 5, 2022 letter from Defendant to the Washington Attorney General states that "Affected documents included names, addresses, social security numbers, and, in some cases, dates of birth, and/or driver's license numbers of Washington residents." https://agportal-s3bucket.s3.amazonaws.com/databreach/BreachM13645.pdf (last visited October 14, 2022).

the severity of the risk they now face. For example, a sample notice letter provided to the Maine Attorney General states, in part:

> **WHAT HAPPENED?**
> On December 23, 2021, RRD identified a systems intrusion in our technical environment. We promptly implemented a series of containment measures to address this situation, including activating our incident response protocols, shutting down our servers and systems and commencing a forensic investigation. We took immediate action to isolate the incident. We determined that outside actors first accessed RRD systems on November 29, 2021, but it was not initially clear whether any personal data had been accessed or removed. However, on July 12, 2022, we learned that your personal information appears to have been exfiltrated from our corporate data system.
> …
> **WHAT CAN YOU DO?**
> At this time, we are not aware of any misuse of the information. As a precautionary measure, we encourage all individuals to remain vigilant for incidence of fraud and identity theft by reviewing account statements, monitoring free credit reports, and promptly reporting any suspicious activity.[5]

37. Defendant should have disclosed that "on January 15th, the Conti ransomware gang claimed responsibility and began leaking 2.5GB of data allegedly stolen from RRD."[6] It is difficult to reconcile this fact with Defendant's statement to victims that it is "not aware of any misuse of the information" exfiltrated in the Data Breach.

38. There is a likelihood that more information was accessed and exfiltrated during the approximate month that the attacker was able to access Defendant's system without detection, including, but not limited to, bank account and routing numbers necessary for direct deposits. The information confirmed to be compromised in the Data Breach is also sufficient to bypass many identity verification procedures utilized by banking and financial institutions.

---

[5] Sample Notice Letter available at: https://apps.web.maine.gov/online/aeviewer/ME/40/ad5791f3-1fb7-4c52-bd34-d97802b91f3d.shtml (last visited October 14, 2022).

[6] https://www.bleepingcomputer.com/news/security/marketing-giant-rrd-confirms-data-theft-in-conti-ransomware-attack/ (last visited Oct. 14, 2022).

39. Defendant claims that to prevent a similar occurrence in the future, it implemented measures designed to enhance the monitoring and analysis capabilities of its network. However, details about the purported remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

40. In an apparent attempt to assuage the concerns of victims and regulators, Defendant states in its notice letters that: "While our investigation is complete, remediation efforts have been ongoing since discovery of the intrusion. RRD believes to the best of its knowledge that the intrusion has been removed and effective controls have been further implemented to prevent additional incidents from the attacker."[7] Such mealy-mouthed statements are less than reassuring.

The Conti Ransomware Attack was Foreseeable and Preventable

41. The FBI has been warning companies, such as Defendant, about the threat posed by the Conti ransomware group, and to be on the lookout for attacks from this group, for a year. It issued a Flash Alert about Conti ransomware attacks in May 2021, and a Joint Cybersecurity Advisory on September 22, 2021, approximately two months before this attack took place. The Advisory was disseminated with details about what red flags indicate a business has been compromised by Conti ransomware, and how attacks can be avoided.

42. As early as May 20, 2021, the FBI issued a Flash Alert that detailed the threat posed by the Conti group. It highlighted that "among the more than 400 organizations worldwide victimized by Conti, over 290 of which are located in the U.S. Like most ransomware variants, Conti typically steals victims' files and encrypts the servers and workstations in an effort to force a ransom payment from the victim. The ransom letter instructs victims to contact the actors through

[7] https://oag.ca.gov/system/files/RRD%20Multistate%20Proof.pdf (last visited Oct. 14, 2022).

an online portal to complete the transaction. If the ransom is not paid, the stolen data is sold or published to a public site controlled by the Conti actors."[8]

43. In the initial FBI Flash Alert, the FBI included a lengthy list of recommended mitigations businesses should take to avoid or minimize the effects of a Conti attack, including:

- Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Implement network segmentation.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (i.e., hard drive, storage device, the cloud).
- Install updates/patch operating systems, software, and firmware as soon as they are released.
- Use multifactor authentication where possible.
- Use strong passwords and regularly change passwords to network systems and accounts, implementing the shortest acceptable timeframe for password changes. Avoid reusing passwords for multiple accounts.
- Disable unused remote access/RDP ports and monitor remote access/RDP logs.
- Require administrator credentials to install software.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Install and regularly update anti-virus and anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a VPN.
- Consider adding an email banner to messages coming from outside your organizations.
- Disable hyperlinks in received emails.

[8] FBI Flash: Conti Ransomware Attacks Impact Healthcare and First Responder Networks (May 20, 2021); https://www.ic3.gov/Media/News/2021/210521.pdf

- Focus on cyber security awareness and training.
- Regularly provide users with training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities (i.e., ransomware and phishing scams).[9]

44. Defendant, a multibillion-dollar corporation with troves of sensitive employee data, either knew or should have known, and should have taken steps to prevent, Conti's widely publicized methods of attack.

45. As a result of Defendant's inadequate security and the vast amounts of PII it maintained, Defendant should have recognized that it would be targeted by Conti. Moreover, it has been widely reported that the "ransomware attack came just after announcing [RRD's] definitive merger agreement to be acquired by Chatham Asset Management."[10] The very same month that the attack occurred, "the FBI released a Private Industry Notification warning that ransomware gangs commonly time their attacks to coincide with significant financial events, such as mergers and acquisitions, as leverage to get victims to pay ransoms."

46. The specifics of Conti's attack practices are well documented. Public reports by cybersecurity firms, such as a November 11, 2021 threat analysis report from the Cybereason Global SOC Team, walk readers step by step through Conti's methods of attack and how such attacks can be prevented.[11]

47. Moreover, On September 22, 2021, in continuing efforts to alert businesses and their employees about the growing Conti threat, the FBI and NSA sent out warning about the Conti group over Twitter, with a call to take "immediate action."

---

[9] *Id.*

[10] https://www.bleepingcomputer.com/news/security/marketing-giant-rrd-confirms-data-theft-in-conti-ransomware-attack/ (last visited Oct. 14, 2022).

[11] https://www.cybereason.com/blog/threat-analysis-report-from-shatak-emails-to-the-conti-ransomware (last visited May 19, 2022).

48. On that same day, September 22, 2021, the U.S. Cybersecurity & Infrastructure Security Agency ("CISA"), in conjunction with the FBI and NSA published a Joint Cybersecurity Advisory on Conti Ransomware.[12] These agencies reported that more than 400 Conti ransomware attacks had taken place on U.S. and international organizations. According to these groups, "Conti actors frequently use a double extortion tactic: if the victim refuses to pay for data decryption, the malicious actor threatens to leak the data or sell it for profit."

49. In that Joint Cybersecurity Advisory, CISA provided businesses with a lengthy listing of technical details that explained how the group was gaining initial access to business IT networks, indicators that would let businesses know they had been compromised, techniques used by Conti to compromise IT systems, and yet again, another list of recommended mitigations

[12] See, Joint Cybersecurity Advisory: Conti Ransomware (9/22/21); https://www.cisa.gov/uscert/sites/default/files/publications/AA21-265A-Conti_Ransomware_TLP_WHITE.pdf (last accessed May 24, 2022).

to reduce the risk of compromise from Conti ransomware attacks, with additional mitigations not previously included in the FBI Flash Alert.[13] The 10-page technical treatise also provided references to other helpful materials for businesses with links, and an offer for "Free Cyber Hygiene Services" offered by CISA to help organizations "assess, identify, and reduce their exposure to threats, including ransomware."[14] The increase in such attacks, and the attendant risk of future attacks, was widely known within Defendant's business community. Due to the high-profile nature of these breaches and attacks, Defendant either was or should have been on heightened notice and aware of such attacks and, therefore, should have been on notice of its duty to be proactive in guarding against being subject to such attacks and adequately performed its duty of preparing for and immediately identifying such an attack.

50. Despite the sophistication of Conti and its ransomware, it must still rely on rudimentary tactics for deploying malware on data rich systems, such as basic phishing emails.[15] Such attacks are entirely preventable through proper training of employees to recognize phishing emails in combination with industry standard security measures such as required two-factor or multi-factor authentication to access email accounts and/or other computer systems.

51. Even with a successful initial infection vector through basic phishing techniques, Conti ransomware attacks may be identified and prevented by widely available software, such as the Cyberreason Defense Platform, which is known to "fully detect[] and prevent[] the Conti ransomware."[16]

[13] *Id*.
[14] *Id*. page, 9.
[15] https://www.cybereason.com/blog/research/cybereason-vs.-conti-ransomware (last visited October 14, 2022).
[16] *Id.*

52. Despite the well-known risks, Defendant inexplicably failed to properly train employees, failed to implement industry standard security measures, and maintained highly sensitive employee information in a manner it knew or should have known was vulnerable to access and exfiltration.

53. Despite the prevalence of public announcements of this data breach and data security compromises and despite numerous attempts on the part of the federal government to inform companies like Defendant of the threat posed by ransomware attacks in general and Conti in particular, Defendant was negligent and did not adequately prepare for this wholly foreseeable event, allowing extremely sensitive data to be accessed, viewed and stolen by the Conti ransomware group. Defendant thus breached its duty to take appropriate steps to protect Plaintiffs' and Class Members' PII from being compromised.

54. What is worse, despite Defendant's obligations under the law to promptly notify affected individuals so they can take appropriate action, Defendant failed to promptly provide such notice in the most expedient time possible and without unreasonable delay, failed to include in the Data Breach Notice Letter a sufficient description of the Data Breach, and failed to provide in the Data Breach Notice Letter the information needed by Plaintiffs and other similarly situated individuals to enable them to react appropriately to the Data Breach, including taking whatever mitigation measures are necessary.

55. As a sophisticated Fortune 500 company that collects, utilizes, and stores particularly sensitive PII, Defendant was at all times fully aware of the increasing risks of cyber-attacks targeting the PII they controlled, and its obligation to protect the PII of Plaintiffs and Class Members. This is confirmed by the language of Defendant's Privacy Policy, which recognizes these risks and importance of safeguarding PII.

56. Defendant itself suffered a different data breach approximately 10 years ago that exposed the unencrypted Social Security numbers of United Healthcare customers. According to a sample notice of data breach letter filed by United Healthcare with the California Attorney General on January 28, 2013:

> According to RR Donnelley, a print and mailing vendor that UnitedHealthcare uses, sometime between the second half of September and the end of November, 2012, an unencrypted desktop computer was stolen from one of its facilities. On December 3, 2012, upon discovering that the computer was stolen, the vendor promptly filed a report with law enforcement, and because it was entrusted with UnitedHealthcare member data as part of a Business Associate relationship, UnitedHealthcare was also notified.
>
> According to our vendor, the 2003 information contained on the computer was limited to your name, address and Social Security number. We have no indication that this information has been accessed, misused or further disclosed. The vendor is continuing to work with law enforcement in an attempt to locate the stolen computer.

Defendant Failed to Comply with Federal Trade Commission Data Security Standards

57. Defendant also violated the duties applicable to it under the Federal Trade Commission Act (15 U.S.C. § 45 et seq.) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC, pursuant to that Act, has concluded that a company's failure to maintain reasonable and appropriate data security for sensitive personal information is an "unfair practice" in violation of the FTC Act.

58. As established by these laws, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant also owed a duty to Plaintiffs and Class Members to provide reasonable security in compliance with industry standards and state and federal requirements, and to ensure that its computer systems, networks, and protocols adequately protected this PII and were

not exposed to infiltration. This also included a duty to Plaintiffs and Class Members to design, maintain, and test its computer systems to ensure that the PII was adequately secured and protected; to create and implement reasonable data security practices and procedures to protect the PII in its possession, and avoid access to its systems through processes such as phishing, including adequately training employees and others who accessed information within its systems on how to adequately protect this information and avoid permitting such infiltration such as by use of multi-factor authentication; to implement processes that would detect a breach of its data security systems in a timely manner and to act upon data security warnings and alerts in a timely fashion; to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII; and to disclose in a timely and accurate manner when data breaches or ransomware attacks occurred.

59. Defendant also needed to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems. It is apparent from the data accessed that Defendant did not do so.

60. Defendant owed these duties to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendant affirmatively chose to design these systems with inadequate user authentication, security protocols and privileges, and set up faulty patching and updating protocols. These affirmative decisions resulted in Conti being able to execute the ransomware attack and exfiltrate the data in question, to the injury and detriment of Plaintiffs and Class Members. By taking affirmative acts inconsistent with these obligations that left Defendant's computer systems vulnerable to a ransomware attack, Defendant disclosed and/or permitted the disclosure of PII to unauthorized third parties. Defendant

thus failed to preserve the confidentiality of PII it was duty-bound to protect.

Defendant Failed to Comply with United States Cybersecurity and Infrastructure Standards

61. Additional measures recommended by the United States Cybersecurity & Infrastructure Security Agency include:

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

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

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

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

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

contact information you have for the sender is authentic before you contact them.

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

g. **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.[17]

Defendant Failed to Comply with Basic Industry Standards

62. Defendant also should have followed standard measures recommended by the Microsoft Threat Protection Intelligence Team, including:

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;

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

[17] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last accessed July 11, 2022).

- 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].[18]

63. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above industry standard measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Plaintiffs' and Class Members' PII.

PII is Very Valuable

64. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[19] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[20]

---

[18] *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 accessed Aug. 23, 2021).
[19] 17 C.F.R. § 248.201 (2013).
[20] *Id*.

65. There is a robust criminal market for the type of PII at issue here. Such PII has high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[21] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[22] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[23]

66. There is also a robust legitimate market for the type of sensitive information at issue here. Marketing firms utilize personal information to target potential customers, and an entire economy exists related to the value of personal data.

Theft of PII is Very Hard to Remedy

67. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone

[21] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 10, 2022).

[22] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed July 10, 2022).

[23] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed July 11, 2022).

> illegally using your Social Security number and assuming your identity can cause a lot of problems.[24]

68. It is not easy—or often possible—to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

69. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The 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."[25]

70. The information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security numbers and names.

71. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the

[24] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed July 10, 2022).
[25] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed July 10, 2022).

black market."[26]

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

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[27]

74. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Plaintiffs' and Class Members' PII, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

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

76. Despite the risk faced by Plaintiffs and Class Members as a result of the exfiltration of their valuable PII, Defendant has only offered Plaintiffs and Class Members a limited 12-month

---

[26] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed July 10, 2022).

[27] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed July 11, 2022).

subscription to identity and credit monitoring services through Experian. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here. Moreover, Defendant put the burden squarely on Plaintiffs and Class Members to enroll in the inadequate monitoring services.

PLAINTIFFS' EXPERIENCES

Plaintiff Robin Forslund

77. Plaintiff Forslund is a former employee of Defendant.

78. As a condition of Plaintiff's employment, RRD required Plaintiff Forslund to provide it with his PII, including name, address, Social Security numbers, date of birth, and driver's license numbers. Plaintiff Forslund provided his PII to RRD and trusted the company would use reasonable measures to protect the PII according to RRD's internal policies. Upon receipt, Defendant entered Plaintiff Forslund's PII on its network, where it was stored and maintained.

79. Plaintiff Forslund greatly values his privacy, especially PII such as Social Security number. Plaintiff Forslund would not have allowed Defendant, or anyone in Defendant's position, to maintain his PII if he believed that Defendant would fail to safeguard that information from unauthorized access and theft.

80. Indeed, Plaintiff Forslund typically takes measures to protect his PII and is very careful about sharing his PII. Plaintiff Forslund has never knowingly transmitted unencrypted PII over the internet or other unsecured source. Plaintiff stores any documents containing his PII in a safe and secure location, and he diligently chooses unique usernames and passwords for his online accounts.

81. Plaintiff Forslund received a Notice letter, dated August 5, 2022, from Defendant informing him that his PII had been compromised in the Data Breach. The Notice letter stated that

Plaintiff's Social Security number and date of birth were accessed and exfiltrated by a criminal group.

82. Plaintiff Forslund 's privacy has been invaded by the access, exfiltration, and theft of his PII, which is now in the hands of criminal third parties.

83. Plaintiff Forslund has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse of his PII resulting from the Data Breach and theft of his PII, especially his Social Security Number.

84. Recognizing the present, immediate, and certainly impending risk of harm Plaintiff Forslund faces, Defendant offered him a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff received also cautioned him to "remain vigilant for incidence of fraud and identity theft by reviewing account statements, [and] monitoring free credit reports."

85. In response to Defendant's Notice Letter and in efforts to mitigate the risk, Plaintiff Forslund spent time dealing with the consequences of the Data Breach, which included time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. Moreover, this time was spent at Defendant's direction by way of the Data Breach notice where Defendant advised Plaintiff Forslund to mitigate his damages by, among other things, monitoring his accounts for fraudulent activity. This time has been lost forever and cannot be recaptured.

86. Plaintiff Forslund also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant for the purpose of obtaining and/or maintaining employment with Defendant.

87. To Plaintiff Forslund's knowledge, his Social Security number and date of birth has not been compromised in a prior data breach.

88. Plaintiff Forslund has suffered and continues to suffer annoyance, interference, and inconvenience as a result of the Data Breach, as well as anxiety and stress caused by the loss of privacy and risk of future harm.

89. Plaintiff Forslund will remain at risk for fraud and identity theft for the foreseeable future, which will require Plaintiff Forslund to spend considerable time and money on an ongoing basis to mitigate and protect against future financial harm.

90. Specifically, the future costs of data and identity theft monitoring services are now reasonable and necessary to prevent or mitigate criminal misuse of Plaintiff Forslund's PII beyond the one year offered by Defendant.

91. Upon information and belief, Plaintiff Forslund's PII remains on Defendant's vulnerable network, placing Plaintiff Forslund at an ongoing risk of harm in future data security incidents. Plaintiff Forslund has a continuing interest in ensuring that his personal information is protected and safeguarded from future breaches that will cause him additional harm.

Plaintiff Timothy Kelly

92. Plaintiff Timothy Kelly is a former employee of Defendant.

93. As a condition of Plaintiff's employment, RRD required Plaintiff Kelly to provide it with his PII, including name, address, Social Security numbers, date of birth, and driver's license numbers. Plaintiff Kelly provided his PII to RRD and trusted the company would use reasonable measures to protect the PII according to RRD's internal policies. Upon receipt, Defendant entered Plaintiff Kelly's PII on its network, where it where it was stored and maintained.

94. Plaintiff Kelly greatly values his privacy, especially PII such as Social Security number. Plaintiff would not have allowed Defendant, or anyone in Defendant's position, to maintain his PII if he believed that Defendant would fail to safeguard that information from

unauthorized access.

95. Plaintiff Kelly typically takes measures to protect his PII and is very careful about sharing his PII. Plaintiff Kelly has never knowingly transmitted unencrypted PII over the internet or other unsecured source. Plaintiff stores any documents containing his PII in a safe and secure location, and he diligently chooses unique usernames and passwords for his online accounts.

96. Plaintiff Kelly received a Notice letter, dated August 5, 2022, from Defendant informing him that his PII had been compromised in the Data Breach. The Notice letter stated that Plaintiff's Social Security number was accessed and exfiltrated by a criminal group.

97. Recognizing the present, immediate, and certainly impending risk of harm Plaintiff Kelly faces, Defendant offered him a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff received also cautioned him to "remain vigilant for incidence of fraud and identity theft by reviewing account statements, [and] monitoring free credit reports."

98. Plaintiff Kelly's privacy has been invaded by the access, exfiltration, and theft of his PII, which is now in the hands of criminal third parties.

99. Plaintiff Kelly has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse of his PII resulting from the Data Breach and theft of his PII, especially his Social Security number.

100. In response to Defendant's Notice Letter and in efforts to mitigate the risk, Plaintiff Kelly spent time dealing with the consequences of the Data Breach, which included time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. Moreover, this time was spent at Defendant's direction by way of the Data Breach notice where Defendant advised Plaintiff Kelly to mitigate his damages by, among other things, monitoring his accounts for fraudulent activity. This time has

been lost forever and cannot be recaptured.

101. Plaintiff Kelly also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant for the purpose of obtaining and/or maintaining employment with Defendant, which was compromised in and as a result of the Data Breach.

102. To Plaintiff's knowledge, his Social Security number has not been compromised in a prior data breach.

103. Plaintiff Kelly has suffered and continues to suffer annoyance, interference, and inconvenience as a result of the Data Breach, as well as anxiety and stress caused by the loss of privacy and risk of future harm.

104. Plaintiff Kelly will remain at risk for fraud and identity theft for the foreseeable future, which will require Plaintiff Kelly to spend considerable time and money on an ongoing basis to mitigate and protect against future financial harm.

105. Specifically, the future costs of data and identity theft monitoring services are reasonable and necessary to prevent or mitigate criminal misuse of Plaintiff Kelly's PII beyond the one year offered to Plaintiff.

106. Upon information and belief, Plaintiff Kelly's PII remains on Defendant's vulnerable network, placing Plaintiff Kelly at an ongoing risk of harm in future data security incidents. Plaintiff Kelly has a continuing interest in ensuring that his personal information is protected and safeguarded from future breaches that will cause him additional harm.

Plaintiff George Lenz

107. Plaintiff Lenz worked as an employee of Defendant's for 13 years and provided his PII to Defendant as a condition of his employment which was then entered into Defendant's

database and maintained by Defendant.

108. Plaintiff Lenz reasonably understood and expected that Defendant would safeguard his PII and timely and adequately notify him in the event of a data breach. Plaintiff Lenz would not have allowed Defendant, or anyone in Defendant's position, to maintain his PII if he believed that Defendant would fail to safeguard that information from unauthorized access.

109. Plaintiff Lenz received a Notice letter dated August 5, 2022, from Defendant informing him that his PII had been compromised in the Data Breach. The Notice letter stated that Plaintiff Lenz's Social Security Number was accessed and exfiltrated by a criminal group. This Notice letter directly contradicted what Plaintiff Lenz had been told by Defendant when working for the company.

110. Recognizing the present, immediate, and certainly impending risk of harm Plaintiff Lenz faces, Defendant offered him a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Lenz received also cautioned him to "remain vigilant for incidence of fraud and identity theft by reviewing account statements, [and] monitoring free credit reports."

111. Plaintiff Lenz greatly values his privacy and PII and takes reasonable steps to maintain the confidentiality of his PII. Plaintiff Lenz is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

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

113. As a result of the Data Breach, Plaintiff Lenz has spent approximately 20-25 hours researching the Data Breach, verifying the legitimacy of the Notice letter, signing up for the credit

monitoring service, reviewing his bank accounts, monitoring his credit report, changing his passwords and payment account numbers, and other necessary mitigation efforts. This is valuable time Plaintiff spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

114. The Data Breach has caused Plaintiff Lenz to suffer fear, anxiety, and stress, which has been compounded by Defendant's nine-month delay in noticing him of the fact that his Social Security number in conjunction with his date of birth were acquired by criminals as a result of the Data Breach.

115. Plaintiff Lenz 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 Lenz will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

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

Plaintiff Matthew Menting

117. Plaintiff Menting is a former RRD employee, having worked for the company between 2016-2017 and again between 2017-October 2018.

118. As a condition of Plaintiff Menting's employment, RRD required Plaintiff Menting to provide it with their PII, including name, address, Social Security numbers, date of birth, and driver's license numbers. Plaintiff Menting provided their PII to RRD and trusted the company would use reasonable measures to protect the PII according to RRD's internal policies. Upon

receipt, Defendant entered Plaintiff Menting's PII on its network, where it was stored and maintained.

119. Plaintiff Menting greatly values their privacy, especially PII such as their Social Security number. Plaintiff Menting would not have allowed Defendant, or anyone in Defendant's position, to maintain their PII if they believed that Defendant would fail to safeguard that information from unauthorized access.

120. Plaintiff Menting typically takes measures to protect their PII and is very careful about sharing their PII. Plaintiff has never knowingly transmitted unencrypted PII over the internet or other unsecured source. Plaintiff stores any documents containing their PII in a safe and secure location, and they diligently choose unique usernames and passwords for their online accounts.

121. Plaintiff Menting received a Notice letter dated August 5, 2022, from Defendant informing them that their PII had been compromised in the Data Breach. The Notice letter stated that Plaintiff's Social Security number was accessed and exfiltrated by a criminal group.

122. Recognizing the present, immediate, and certainly impending risk of harm Plaintiff Menting faces, Defendant offered them a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Menting received also cautioned them to "remain vigilant for incidence of fraud and identity theft by reviewing account statements, [and] monitoring free credit reports."

123. Plaintiff Menting's privacy has been invaded by the access, exfiltration, and theft of their PII, which is now in the hands of criminal third parties.

124. Plaintiff Menting has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse of their PII resulting from the Data Breach and theft of their PII, especially their Social Security Number.

125. In response to Defendant's Notice Letter and in efforts to mitigate the risk, Plaintiff

Menting spent time dealing with the consequences of the Data Breach, which included time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring their accounts and credit reports to ensure no fraudulent activity has occurred. Moreover, this time was spent at Defendant's direction by way of the Data Breach notice where Defendant advised Plaintiff Menting to mitigate their damages by, among other things, monitoring their accounts for fraudulent activity. This time has been lost forever and cannot be recaptured.

126. Plaintiff Menting also suffered actual injury in the form of damages to and diminution in the value of their PII—a form of intangible property that he entrusted to Defendant for the purpose of obtaining and/or maintaining employment with Defendant, which was compromised in and as a result of the Data Breach.

127. To Plaintiff Menting's knowledge, their Social Security number has not been compromised in a prior data breach.

128. Plaintiff Menting has suffered and continues to suffer annoyance, interference, and inconvenience as a result of the Data Breach, as well as anxiety and stress caused by the loss of privacy and risk of future harm.

129. Plaintiff Menting will remain at risk for fraud and identity theft for the foreseeable future, which will require Plaintiff Menting to spend considerable time and money on an ongoing basis to mitigate and protect against future financial harm.

130. Specifically, the future costs of data and identity theft monitoring services are reasonable and necessary to prevent or mitigate criminal misuse of Plaintiff Menting's PII beyond the one year offered to Plaintiff Menting.

131. Upon information and belief, Plaintiff Menting's PII remains on Defendant's vulnerable network, placing Plaintiff Menting at an ongoing risk of harm in future data security

incidents. Plaintiff Menting has a continuing interest in ensuring that their personal information is protected and safeguarded from future breaches.

Plaintiff Donalyn North

132. Plaintiff Donalyn North is a former employee of Defendant. Plaintiff North provided her PII to Defendant as a condition of her employment which was then entered into Defendant's database and maintained by Defendant. Plaintiff North has not worked for Defendant for approximately eight (8) years.

133. Plaintiff North reasonably understood and expected that Defendant would safeguard her PII, and timely and adequately notify her in the event of a data breach. Plaintiff North would not have allowed Defendant, or anyone in Defendant's position, to maintain her PII if she believed that Defendant would fail to safeguard that information from unauthorized access.

134. Plaintiff North received a Notice letter dated August 5, 2022 from Defendant informing her that her PII had been compromised in the Data Breach. The Notice letter stated that Plaintiff North's Social Security number, date of birth, and bank account number were accessed and exfiltrated by a criminal group.

135. Recognizing the present, immediate, and certainly impending risk of harm Plaintiff North faces, Defendant offered her a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff North received also cautioned her to "remain vigilant for incidence of fraud and identity theft by reviewing account statements, [and] monitoring free credit reports."

136. Plaintiff North greatly values her privacy and PII and takes reasonable steps to maintain the confidentiality of her PII. Plaintiff North is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

137. Plaintiff North stores any and all documents containing PII in a secure location and

destroys any documents she receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

138. To Plaintiff North's knowledge, her Social Security number has not been compromised in a prior data breach.

139. As a result of the Data Breach, Plaintiff North has spent approximately two (2) hours researching the Data Breach, verifying the legitimacy of the Notice letter, reviewing her bank accounts, and monitoring her credit report. This is valuable time Plaintiff North spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

140. The Data Breach has caused Plaintiff North to suffer fear, anxiety, and stress, which has been compounded by Defendant's nine-month delay in noticing her of the fact that her Social Security number in conjunction with her date of birth were acquired by criminals as a result of the Data Breach.

141. Plaintiff North 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 North will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

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

Plaintiff Eric Ottenheimer

143. Plaintiff Ottenheimer is a former RRD employee. As a condition of Plaintiff Ottenheimer's employment, RRD required Plaintiff Ottenheimer to provide it with his PII, including name, address, Social Security number, date of birth, and driver's license number. Plaintiff Ottenheimer provided his PII to RRD and trusted the company would use reasonable measures to protect the PII according to RRD's internal policies, industry standards, as well as state and federal law. Upon receipt, Defendant entered Plaintiff Ottenheimer's PII on its network, where it was stored and maintained.

144. Plaintiff Ottenheimer greatly values his privacy, especially PII such as his Social Security number. Plaintiff would not have allowed Defendant, or anyone in Defendant's position, to maintain his PII if he believed that Defendant would fail to safeguard that information from unauthorized access.

145. Plaintiff Ottenheimer typically takes measures to protect his PII and is very careful about sharing his PII. Plaintiff has never knowingly transmitted unencrypted PII over the internet or other unsecured source. Plaintiff stores any documents containing his PII in a safe and secure location, and he diligently chooses unique usernames and passwords for his online accounts.

146. Plaintiff Ottenheimer received a Notice letter, dated August 5, 2022, from Defendant informing him that his PII had been compromised in the Data Breach. The Notice letter stated that Plaintiff's Social Security number was accessed and exfiltrated by a criminal group.

147. Recognizing the present, immediate, and certainly impending risk of harm Plaintiff faces, Defendant offered him a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff received also cautioned him to "remain vigilant for incidence of fraud and identity theft by reviewing account statements, [and] monitoring free credit reports."

148. Plaintiff Ottenheimer's privacy has been invaded by the access, exfiltration, and theft of his PII, which is now in the hands of criminal third parties.

149. Plaintiff Ottenheimer has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse of his PII resulting from the Data Breach and theft of his PII, especially his Social Security number.

150. In response to Defendant's Notice Letter and in efforts to mitigate the risk, Plaintiff Ottenheimer spent approximately three (3) hours researching the Data Breach, verifying the legitimacy of the Notice letter, signing up for the credit monitoring service, reviewing his bank accounts, monitoring his credit report, implementing a credit freeze, and other necessary mitigation efforts. This is valuable time Plaintiff spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation. Moreover, this time was spent at Defendant's direction by way of the Data Breach notice where Defendant advised Plaintiff to mitigate her damages by, among other things, monitoring their accounts for fraudulent activity. This time has been lost forever and cannot be recaptured.

151. Plaintiff Ottenheimer's wife also spent approximately one hour (including travel time) at their local bank branch to discuss the fact that Plaintiff Ottenheimer's PII was involved in a data breach and to confirm that they had not yet experienced bank fraud or theft as a result. Plaintiff Ottenheimer's wife used their family's vehicle and gasoline to travel to and from the bank, costing them gas money and placing wear and tear on their vehicle.

152. Plaintiff Ottenheimer also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant for the purpose of obtaining and/or maintaining employment with Defendant, which was compromised in and as a result of the Data Breach.

153. To Plaintiff Ottenheimer's knowledge, his Social Security number has not been compromised in a prior data breach.

154. Plaintiff Ottenheimer has suffered and continues to suffer annoyance, interference, and inconvenience as a result of the Data Breach, as well as anxiety and stress caused by the loss of privacy and risk of future harm.

155. Plaintiff Ottenheimer will remain at risk for fraud and identity theft for the foreseeable future, which will require Plaintiff to spend considerable time and money on an ongoing basis to mitigate and protect against future financial harm.

156. Specifically, the future costs of data and identity theft monitoring services are reasonable and necessary to prevent or mitigate criminal misuse of Plaintiff Ottenheimer's PII beyond the one year offered by Defendant.

157. Upon information and belief, Plaintiff Ottenheimer's PII remains on Defendant's vulnerable network, placing Plaintiff and at an ongoing risk of harm in future data security incidents. Plaintiff has a continuing interest in ensuring that his personal information is protected and safeguarded from future breaches.

Plaintiff Robin Rector

158. Plaintiff Rector is a former RRD employee. As a condition of Plaintiff Rectors's employment, RRD required Plaintiff to provide it with her PII, including name, address, Social Security numbers, date of birth, and driver's license numbers. Plaintiff Rector provided her PII to RRD and trusted the company would use reasonable measures to protect the PII according to RRD's internal policies, industry standards, as well as state and federal law. Upon receipt, Defendant entered Plaintiff Rector's PII on its network, where it was maintained following his employment.

159. Plaintiff Rector greatly values her privacy, especially PII such as Social Security number. Plaintiff would not have allowed Defendant, or anyone in Defendant's position, to maintain her PII if she believed that Defendant would fail to safeguard that information from unauthorized access.

160. Plaintiff Rector typically takes measures to protect his PII and is very careful about sharing her PII. Plaintiff has never knowingly transmitted unencrypted PII over the internet or other unsecured source. Plaintiff stores any documents containing her PII in a safe and secure location, and he diligently chooses unique usernames and passwords for his online accounts.

161. Plaintiff Rector received a Notice letter, dated August 5, 2022, from Defendant informing her that her PII had been compromised in the Data Breach. The Notice letter stated that Plaintiff's Social Security number was accessed and exfiltrated by a criminal group.

162. Recognizing the present, immediate, and certainly impending risk of harm Plaintiff Rector faces, Defendant offered her a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff received also cautioned her to "remain vigilant for incidence of fraud and identity theft by reviewing account statements, [and] monitoring free credit reports."

163. Plaintiff Rector 's privacy has been invaded by the access, exfiltration, and theft of her PII, which is now in the hands of criminal third parties.

164. Plaintiff Rector has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse of her PII resulting from the Data Breach and theft of her PII, especially her Social Security number.

165. In response to Defendant's Notice Letter and in efforts to mitigate the risk, Plaintiff Rector spent time dealing with the consequences of the Data Breach, which included time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts and credit

reports to ensure no fraudulent activity has occurred. Moreover, this time was spent at Defendant's direction by way of the Data Breach notice where Defendant advised Plaintiff Rector to mitigate her damages by, among other things, monitoring her accounts for fraudulent activity. This time has been lost forever and cannot be recaptured.

166. Moreover, Plaintiff Rector has suffered actual identity theft and related monetary damages. Within a week of receiving the notice from RRD, Plaintiff Rector experienced fraudulent charges on her bank and credit card accounts totaling approximately $800. As a result, Plaintiff Rector incurred overdraft charges on her bank account, which then precluded her paying her electricity bill, forcing her to incur late fees.

167. Plaintiff Rector was also required to cancel her credit card and bank accounts, leaving her without access to her funds until new accounts were set up. To cancel the bank accounts, she was required travel to the bank to resolve issues, which caused her to incur travel costs with gasoline charges and mileage.

168. Plaintiff Rector also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that he entrusted to Defendant for the purpose of obtaining and/or maintaining employment with Defendant, which was compromised in and as a result of the Data Breach.

169. To Plaintiff Rector's knowledge, her Social Security number has not been compromised in a prior data breach.

170. Plaintiff Rector has suffered and continues to suffer annoyance, interference, and inconvenience as a result of the Data Breach, as well as anxiety and stress caused by the loss of privacy and risk of future harm.

171. Plaintiff Rector will remain at risk for fraud and identity theft for the foreseeable

future, which will require Plaintiff to spend considerable time and money on an ongoing basis to mitigate and protect against future financial harm.

172. Specifically, the future costs of data and identity theft monitoring services are reasonable and necessary to prevent or mitigate criminal misuse of her PII beyond the one year offered by Defendant.

173. Upon information and belief, Plaintiff Rector's PII remains on Defendant's vulnerable network, placing Plaintiff and at an ongoing risk of harm in future data security incidents. Plaintiff has a continuing interest in ensuring that her personal information is protected and safeguarded from future breaches.

Plaintiff Gail Rossi

174. Plaintiff Rossi is a former RRD employee, having worked for the company in the early 2000s.

175. As a condition of Plaintiff Rossi 's employment, RRD required Plaintiff to provide it with her PII, including name, address, Social Security numbers, date of birth, and driver's license numbers. Plaintiff Rossi provided her PII to RRD and trusted the company would use reasonable measures to protect the PII according to RRD's internal policies. Defendant entered Plaintiff Rossi's PII on its network, where it was stored and maintained.

176. Plaintiff Rossi greatly values her privacy, especially PII such as her Social Security number. Plaintiff would not have allowed Defendant, or anyone in Defendant's position, to maintain her PII if she believed that Defendant would fail to safeguard that information from unauthorized access.

177. Indeed, Plaintiff Rossi typically takes measures to protect her PII and is very careful about sharing her PII. Plaintiff Rossi has never knowingly transmitted unencrypted PII over the

internet or other unsecured source. Plaintiff stores any documents containing her PII in a safe and secure location, and she diligently chooses unique usernames and passwords for her online accounts.

178. Plaintiff Rossi received a Notice letter, dated August 5, 2022, from Defendant informing her that her PII had been compromised in the Data Breach. The Notice letter stated that Plaintiff's name, address, Social Security numbers, date of birth, and driver's license number were accessed and exfiltrated by a criminal group.

179. Plaintiff Rossi's privacy has been invaded by the access, exfiltration, and theft of her PII, which is now in the hands of criminal third parties.

180. Plaintiff Rossi has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse of her PII resulting from the Data Breach and theft of her PII, especially her Social Security number.

181. Recognizing the present, immediate, and certainly impending risk of harm Plaintiff Rossi faces, Defendant offered her a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Rossi received also cautioned her to "remain vigilant for incidence of fraud and identity theft by reviewing account statements, [and] monitoring free credit reports."

182. In response to Defendant's Notice Letter and in efforts to mitigate the risk, Plaintiff spent time dealing with the consequences of the Data Breach, which included time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. Moreover, this time was spent at Defendant's direction by way of the Data Breach notice where Defendant advised Plaintiff to mitigate her damages by, among other things, monitoring her accounts for fraudulent activity. This time has been lost forever and cannot be recaptured.

183. Since receiving the breach notice, Plaintiff Rossi has experienced multiple instances of actual identity theft and fraud. Notably, Plaintiff Rossi received a communication from Alaska Federal Credit Union, a bank that Plaintiff Rossi has never used, stating that it was blocking her account. Plaintiff Rossi also received a notice from Credit Karma stating that someone had changed her password. That password change was not done by Plaintiff Rossi.

184. Plaintiff Rossi spent a significant amount of time dealing with these reports of fraud.

185. Plaintiff Rossi also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant for the purpose of obtaining and/or maintaining employment with Defendant, which was compromised in and as a result of the Data Breach.

186. To Plaintiff Rossi's knowledge, her name, address, Social Security numbers, date of birth, and driver's license number have not been compromised in another data breach.

187. Plaintiff Rossi has suffered and continues to suffer annoyance, interference, and inconvenience as a result of the Data Breach, as well as anxiety and stress caused by the loss of privacy and risk of future harm.

188. Plaintiff Rossi will remain at risk for fraud and identity theft for the foreseeable future, which will require Plaintiff to spend considerable time and money on an ongoing basis to mitigate and protect against future financial harm.

189. Specifically, the future costs of data and identity theft monitoring services are now reasonable and necessary to prevent or mitigate criminal misuse of Plaintiff Rossi's PII beyond the one year offered by Defendant.

190. Upon information and belief, Plaintiff Rossi's PII remains on Defendant's

vulnerable network, placing Plaintiff Rossi and at an ongoing risk of harm in future data security incidents. Plaintiff has a continuing interest in ensuring that her personal information is protected and safeguarded from future breaches that will cause her additional harm.

Plaintiff Gregory Williams

191. Plaintiff Williams is a former employee of Defendant. His employment with RRD ended in approximately 2014. Plaintiff Williams provided his PII to Defendant as a condition of his employment which was then entered into Defendant's database and maintained by Defendant.

192. Plaintiff Williams reasonably understood and expected that Defendant would safeguard his PII and timely and adequately notify him in the event of a data breach. Plaintiff Williams would not have allowed Defendant, or anyone in Defendant's position, to maintain his PII if he believed that Defendant would fail to safeguard that information from unauthorized access.

193. Plaintiff Williams received a Notice letter dated August 5, 2022 from Defendant informing him that his PII had been compromised in the Data Breach. The Notice letter stated that Plaintiff Williams's Date of Birth and Social Security Number were accessed and exfiltrated by a criminal group.

194. Recognizing the present, immediate, and certainly impending risk of harm Plaintiff Williams faces, Defendant offered him a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Williams received also cautioned him to "remain vigilant for incidence of fraud and identity theft by reviewing account statements, [and] monitoring free credit reports."

195. Plaintiff Williams greatly values his privacy and PII and takes reasonable steps to maintain the confidentiality of his PII. Plaintiff Williams is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

196. Plaintiff Williams stores any and all documents containing PII in a secure location and destroys any documents he receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

197. To Plaintiff Williams's knowledge, his Social Security number has not been compromised in a prior data breach.

198. As a result of the Data Breach, Plaintiff Williams has spent approximately 10 hours researching the Data Breach, verifying the legitimacy of the Notice letter, signing up for the credit monitoring service, reviewing his bank accounts, monitoring his credit report, changing his passwords and payment account numbers, instituting a credit freeze, and other necessary mitigation efforts. This is valuable time Plaintiff spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

199. The Data Breach has caused Plaintiff Williams to suffer fear, anxiety, and stress, which has been compounded by Defendant's nine-month delay in noticing him of the fact that his Social Security number in conjunction with his date of birth were acquired by criminals as a result of the Data Breach. Plaintiff Williams recalls that in the weeks immediately following receipt of the Notice Letter, he lost sleep and would wake up thinking of worst-case identity theft scenarios.

200. Plaintiff Williams 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 Williams will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

201. Plaintiff Williams suffers a present injury from the existing and continuing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

Plaintiff Williams has a continuing interest in ensuring that his PII, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

202. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

203. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> **All persons Defendant identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

204. Plaintiff Lenz also seeks to represent a subclass of New York residents (the "New York Subclass") defined as follows:

> **All New York residents that Defendant identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

205. Excluded from the Class and Subclass are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

206. Plaintiffs reserve the right to modify or amend the definition of the proposed class and/or create additional subclasses before the Court determines whether certification is appropriate.

207. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder

of all members is impracticable. Upon information and belief, there are thousands of individuals whose PII was exfiltrated in the Data Breach, and each Class is apparently identifiable within Defendant's records.

208. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exists and predominates over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect Plaintiffs' and Class Members' PII;

b. Whether Defendant had duties not to disclose the Plaintiffs' and Class Members' PII to unauthorized third parties;

c. Whether Defendant had duties not to use Plaintiffs' and Class Members' PII for non-business purposes;

d. Whether Defendant failed to adequately safeguard Plaintiffs' and Class Members' PII;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. 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;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which

permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and Class Members' PII;

k. Whether Defendant violated the consumer protection statutes invoked herein;

l. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

m. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

n. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

209. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

210. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

211. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no

relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

212. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

213. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be

unnecessary and duplicative of this litigation.

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

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

216. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

217. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

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

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. 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;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and Class Members' PII; and/or

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

219. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 218.

220. Plaintiffs and the Class entrusted Defendant with their PII.

221. Plaintiffs and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

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

223. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

224. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiffs and the Classes in Defendant's possession was adequately secured and protected.

225. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain pursuant to regulations.

226. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiffs and the Class.

227. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant.

228. Defendant also had an independent duty under 815 Ill. Comp. Stat. § 530/45(a), which requires data collectors to "implement and maintain reasonable security measures to protect" records from "unauthorized access, acquisition, destruction, use, modification, or disclosure."

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

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

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

232. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiffs and the Class, including basic encryption techniques freely available to Defendant.

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

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

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

236. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and the Class.

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

238. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the Class during the time the PII was within Defendant's possession or control.

239. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

240. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiffs and the Class in the face of increased risk of theft.

241. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of PII.

242. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII they were no longer required to retain pursuant to regulations.

243. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and the Class the existence and scope of the Data Breach.

244. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the PII of Plaintiffs and the Class would not have been compromised.

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

246. Additionally, 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 PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

247. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

248. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se.

249. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to protect.

250. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

251. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiffs and the Class have suffered and will suffer injury, including, but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiffs and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

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

253. Additionally, as a direct and proximate result of Defendant's negligence and negligence per se, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further

unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

254. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Nationwide Class)

255. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 218.

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

257. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiffs' and Class Member's PII.

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

259. Defendant breached the implied contracts they made with Plaintiffs and the Class by failing to adequately safeguard and protect their personal information, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

260. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

261. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Nationwide Class)

262. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 218.

263. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

264. Plaintiffs and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII.

265. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII.

266. Moreover, Defendant retained the PII with no legitimate employment purpose.

267. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

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

269. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

270. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant or had requested that the PII be deleted upon termination of the employment relationship.

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

272. As a direct and proximate result of Defendant's conduct, As a direct result of the Data Breach, Plaintiffs and Class Members have suffered the following actual and imminent injuries: (i) invasion of privacy; (b) monetary harms, including out-of-pocket expenses, loss-of time, and loss of productivity incurred mitigating the present risk and imminent threat of identity theft; (c) actual identity theft and fraud resulting in additional monetary damages; (d) diminution of value of their PII; (e) anxiety, stress, nuisance, and annoyance; (vi) increased targeted and fraudulent robocalls and phishing email attempts; (vii) the present and continuing risk of identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or

criminals; (ix) the retention of the reasonable value of the PII entrusted to Defendant; and (x) the present and continued risk to PII, which remains on Defendant's vulnerable network, placing Plaintiffs and Class Members at an ongoing risk of harm.

273. 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.

274. 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 IV
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Nationwide Class)

275. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 218.

276. Plaintiffs assert a common law claim for invasion of privacy based on Defendant's intrusion upon Plaintiffs' and Class Members' seclusion, and separately, for the public disclosure of private facts to the public at large.

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

278. Defendant owed a duty to Plaintiffs and Class Members to keep their PII confidential.

279. Defendant knowingly implemented data security measures that were less than adequate to reasonably safeguard PII from foreseeable threats.

280. Defendant affirmatively and recklessly disclosed Plaintiffs' and Class Members' PII to unauthorized third-parties after failing to recognize and then responding to a foreseeable phishing attack.

281. Upon information and belief, the PII stolen in the Data Breach is now—or at the very least was—available to the public at large on the dark web. For example, it has been widely reported that following the breach, Conti leaked 2.5 gigabytes of PII to the internet.

282. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiffs' and Class Members' PII is highly offensive to a reasonable person.

283. Defendant's reckless and negligent failure to protect Plaintiffs' and Class Members' PII constitutes an intentional interference with Plaintiffs' and the Class Members' 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.

284. Defendant knowingly did not notify Plaintiffs and Class Members in a timely fashion about the Data Breach.

285. Because Defendant failed to properly safeguard Plaintiffs' and Class Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

286. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII is still maintained by Defendant with its inadequate cybersecurity system and policies.

287. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A

judgment for monetary damages will not end Defendant's inability to safeguard Plaintiffs' and the Class's PII.

288. Plaintiffs have been injured from the invasion of their privacy.

289. Plaintiffs, on behalf of themselves and Class Members, seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' PII.

290. Plaintiffs, on behalf of themselves and Class Members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT V
VIOLATIONS OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT
815 Ill. Comp. Stat. §§ 505/1, *et seq*.
(On behalf of Plaintiffs and the Nationwide Class)

291. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 218.

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

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

294. Even if Plaintiffs are not "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e), Plaintiffs may bring claims under the ICFA because there is a "consumer nexus" between Plaintiffs

and consumers with respect to Defendant's unfair and deceptive trade practices.

295. Plaintiffs' actions were akin to a consumer's action because they justifiably relied on Defendant's public statements and omissions regarding its data security practices. Specifically, Defendant's statements, including its privacy policy, states Defendant will use reasonable security measures to protect its network from cybercriminals and ransomware attacks.

296. Defendant's representations and omissions as to its data security measures, and its failure to implement and maintain reasonable data security measures, concern all individuals because a reasonable consumer, akin to Plaintiffs, does or is reasonably likely to rely on these statements in providing their PII.

297. Defendant's conduct involved consumer protection concerns because Defendant represented to consumers and employees (current and former) that it employed proper data security measures but, in fact, did not. Defendant's conduct also involves consumer protection concerns because Defendant's failure to implement and maintain reasonable data security measures enabled the Conti Group to access and exfiltrate the PII of both employees and consumers from its network. In turn, Plaintiffs' and Class Members' PII is on the dark web.

298. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the CFA, including: (i) failing to maintain adequate data security to keep Plaintiffs' and the Class Members' sensitive PII from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (ii) failing to disclose or omitting materials facts to Plaintiffs and the Class regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the PII of Plaintiffs and the Class; (iii) failing to disclose or omitting materials

facts to Plaintiffs and the Class about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII of Plaintiffs and the Class; and (iv) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs' and the Class's PII and other personal information from further unauthorized disclosure, release, data breaches, and theft.

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

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

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

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

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

304. As a direct and proximate result of Defendant's violations of the CFA, Plaintiffs and the Class have suffered harm: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (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 PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in its 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 PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

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

306. The requested relief by Plaintiffs will assist consumers because it will require Defendant to enhance its data security practices. Specifically, the Complaint seeks injunctive relief via enhanced data security measures. Moreover, any monetary compensation will deter Defendant from additional and future data breach incidents.

COUNT VI
VIOLATION OF NEW YORK LABOR LAW § 203-d
(on behalf of Plaintiff Lenz and the New York Subclass)

307. Plaintiff Lenz ("Plaintiff" for the purposes of this Count) re-alleges and

incorporates by reference paragraphs 1 through 218 in the Complaint as if fully set forth herein. This count is brought on behalf of the New York Subclass (the "Subclass" or "Class" for the purposes of this Count).

308. Plaintiff brings this claim pursuant to the implied private right of action in N.Y. Labor Law § 203–d, or alternatively, as a claim for negligence *per se*. *See Sackin v. TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 752 (S.D.N.Y. 2017).

309. Plaintiff, as a former employee, is within the class of individuals the statute is intended to protect.

310. Pursuant to New York Labor Law Sec.203-D, an employer shall not, unless otherwise required by law:

a. Publicly post or display an employees social security number;

b. Place social security number in files with unrestricted access; or

c. Communicate an employee's personal identifying information to the general public.

311. Defendant failed to provide reasonable security, safeguards, policies, and procedures, and protections to the personal data of Plaintiff and Subclass members, instead permitting unauthorized third parties unrestricted access to Plaintiff's and Subclass members' PII. As a result, Plaintiff's and Subclass members' PII was disclosed to the general public.

312. As a direct and proximate result of Defendant's knowing acts and omissions, Plaintiffs' and the Class's PII was disclosed to unauthorized third parties causing damage to Plaintiff and the Class.

313. Plaintiff and the Class seek relief under New York Labor Law § 203-d, including actual damages, statutory damages, injunctive relief, and/or attorneys' fees, expenses, and costs.

COUNT VII
DECLARATORY JUDGMENT/INJUNTIVE RELIEF
(on behalf of Plaintiffs and the Nationwide Class)

314. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 218.

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

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

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

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

319. To Plaintiffs' knowledge, Defendant has made no changes to its data storage or security practices relating to the PII.

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

321. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury

and lack an adequate legal remedy in the event of another data breach at RRD. The risk of another such breach is real, immediate, and substantial.

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

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

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

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

b) Engaging third-party security auditors and internal personnel to run automated security monitoring;

c) Auditing, testing, and training its security personnel regarding any new or modified procedures;

d) Purging, deleting, and destroying PII not necessary for its provisions of services in a reasonably secure manner;

e) Conducting regular database scans and security checks; and

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs 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' PII, 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 consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

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

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

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

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

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

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

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

DEMAND FOR JURY TRIAL

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

Date: October 14, 2022

Respectfully Submitted,

/s/ *Joseph M. Lyon*
Joseph M. Lyon (OH BAR #76050)
THE LYON LAW FIRM, LLC
2754 Erie Ave.
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
221 West Monroe Street, Suite 2100
Chicago, IL 60606
866.252.0878
gklinger@milberg.com

Raina C. Borrelli
Samuel J. Strauss
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone (608) 237-1775
Facsimile: (608) 509-4423

raina@turkestrauss.com
sam@turkestrauss.com

Terence R. Coates
Jonathan T. Deters
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Telephone: 513.651.3700
Facsimile: 513.665.0219
tcoates@msdlegal.com
jdeters@msdlegal.com

Bryan L. Bleichner
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com

Counsel for Plaintiffs and Putative Class