IN THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF TEXAS HOUSTON DIVISION

JANIE MARCAUREL and SHELBY INGRAM, individually and on behalf of all others similarly situated, Plaintiffs, v. USA WASTE-MANAGEMENT RESOURCES, LLC, and WASTE MANAGEMENT, INC., Defendants.	Case No. 4:21-cv-2027 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Janie Marcaurel and Shelby Ingram ("Plaintiffs"), as individuals and on behalf of all others similarly situated, bring this Class Action Complaint against USA Waste-Management Resources, LLC ("WMR") and Waste Management, Inc. ("WMI" and, collectively, "Defendants" or "WM"), and allege, upon personal knowledge as to their own actions and their counsels' investigations and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard personally identifiable information that Defendants required from their employees as a condition of employment, including without limitation, names, Social Security numbers (or National IDs), dates of birth, and driver's license numbers (collectively, "PII").[1]

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII is also generally defined to include certain identifiers that

Plaintiffs also allege Defendants failed to provide timely, accurate, and adequate notice to Plaintiffs and similarly situated current and former employees and their dependents (collectively, "Class members") that their PII had been lost and precisely what types of information was unencrypted and in the possession of unknown third parties.

2. Part of the bargain of obtaining a job requires turning over to employers valuable PII, including names, Social Security numbers (or National IDs), dates of birth, and driver's license numbers. Identity thieves can use this highly sensitive information to fraudulently open new accounts, access existing accounts, perpetrate identity fraud or impersonate victims in myriad schemes, all of which can cause grievous financial harm, negatively impact the victim's credit scores for years, and cause victims to spend countless hours mitigating the impact.

3. Every year millions of Americans have their most valuable PII stolen and sold online because of data breaches. Despite the dire warnings about the severe impact of data breaches on Americans of all economic strata, companies still fail to put adequate security measures in place to protect their customers' and employees' data.

4. Defendant WMI boasts that it "value[s] safety" and is one of the "world's most ethical companies," yet has failed to meet its obligation to protect the sensitive PII entrusted to it by its more than 45,000 current and former employees.[2]

5. As reported by Defendants, between January 21 and 23, 2021, an unauthorized actor entered the WMI environment and accessed and took a number of files.[3] On May 4, 2021

---

do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number).

[2] https://www.wm.com/us/en/inside-wm/who-we-are, and https://www.wm.com/us/en/inside-wm/who-we-are/awards, last visited June 14, 2021.

[3] *See* Exs. A & B.

and during the weeks following, Defendants determined that the potentially accessed files contained sensitive PII, including data of employees and former employees (and their dependents) such as names, Social Security numbers (or National IDs), dates of birth, and driver's license numbers. Defendants required their employees to provide them with their sensitive PII. Defendants had an obligation to secure that PII by implementing reasonable and appropriate data security safeguards. This was part of the bargain between Plaintiffs and Class members (defined *infra*.) on the one hand and Defendants on the other.

6. As a result of WM's failure to provide reasonable and adequate data security, Plaintiffs' and the Class members' unencrypted, non-redacted PII has been exposed to unauthorized third parties. Plaintiffs and the Class are now at a much higher risk of identity theft and vulnerable to cybercrimes of all kinds, especially considering the highly sensitive PII stolen from WMR.

THE PARTIES

7. Plaintiff Janie Marcaurel is a resident and citizen of California and was employed by Waste Management, Inc. in the Modesto facility in or about 1998 through 1999. Ms. Marcaurel, in connection with her employment, entrusted to Defendants her PII and reasonably believed Defendants would keep her PII secure. Had Defendants disclosed that they would not keep her PII secure and that it would be easily accessible to hackers and third parties, she would have taken additional precautions relating to her PII. She received a *Notice of Data Breach* from WMR dated May 28, 2021, on or about that date.

8. Plaintiff Shelby Ingram is a resident and citizen of Arizona and was employed by Waste Management Natural Services, an affiliate of Defendant WMI, in Phoenix, Arizona in or about June 29, 2015 through January 19, 2021. Ms. Ingram, in connection with her employment,

entrusted to Defendants her PII and reasonably believed Defendants would keep her PII secure. Had Defendants disclosed that they would not keep her PII secure and that it would be easily accessible to hackers and third parties, she would have taken additional precautions relating to her PII. She received a *Notice of Data Breach* from WMR dated May 28, 2021, on or about that date.

9. Defendant USA Waste-Management Resources, LLC ("WMR") is a New York limited liability company with its principal place of business in Houston, Texas. Upon information and belief, WMR's sole member is Defendant Waste Management, Inc. ("WMI"), whose citizenship is stated below. WMR is a subsidiary of and controlled by Defendant WMI.

10. Defendant Waste Management, Inc. ("WMI") is incorporated in Delaware and headquartered at 800 Capitol Street, Houston, Texas, and its stock is traded on the New York Stock Exchange under the symbol "WM." WMI describes itself as North America's leading provider of comprehensive waste management environmental services, providing services throughout the United States and Canada. WMI partners with its residential, commercial, industrial and municipal customers and the communities they serve to manage and reduce waste at each stage from collection to disposal, while recovering valuable resources and creating clean, renewable energy. WMI's "Solid Waste" business is operated and managed locally by its subsidiaries that focus on distinct geographic areas and provide collection, transfer, disposal, and recycling and resource recovery services. Through its subsidiaries, WMI is also a leading developer, operator and owner of landfill gas-to-energy facilities in the U.S. It employed approximately 48,250 people as of December 31, 2020. WMI owns or operates 268 landfill sites, which is the largest network of landfills in the U.S. and Canada. WMI manages 348 transfer stations that consolidate, compact and transport waste. WMI also uses waste to create energy, recovering the gas produced naturally as waste decomposes in landfills and using the gas in generators to make electricity. WMI is a

leading recycler in the U.S. and Canada, handling materials that include cardboard, paper, glass, plastic and metal. It provides recycling programs for municipalities, businesses and households across the U.S. and Canada as well as other services that supplement its Solid Waste business.

JURISDICTION AND VENUE

11. Subject matter jurisdiction in this civil action is authorized pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class members, at least one Class member is a citizen of a state different from that of Defendant, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

12. This Court has personal jurisdiction over Defendants because they are each headquartered in Houston, Texas and they conduct substantial business in this District through their offices and/or affiliates.

13. Venue is likewise proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendants conduct much of their business in this District and Defendants have caused harm to Class members residing in this District.

FACTUAL ALLEGATIONS

A. WM collects and stores thousands of current and former employees' (and their dependents') PII and failed to provide adequate data security to protect it.

14. WM, which is headquartered in Texas with locations in at least 48 states, employs over 45,000 employees, has tens of thousands of former employees, and is a major player in the waste management and recycling industry. WM prides itself on two fundamental commitments and four core values:

- Committed to our people first
- Committed to success with integrity
- Value Inclusion & Diversity

- Value Customers
- Value Safety
- Value our Environment[4]

B. WM's inadequate data security exposed its current and former employees' (and their dependents') sensitive PII.

15. Between January 21 and 23, 2021, an unauthorized actor entered the WM network environment and accessed certain files, including past and current employee files. It was determined that the unauthorized actor accessed names, Social Security number (National ID), date of birth and driver's license number.

16. This incident is referred to herein as the "Data Breach."

17. Plaintiffs each received a letter from WM dated May 28, 2021 (the "Notice Letter," attached hereto as **Exhibit A**), almost four months after the Data Breach occurred. The Notice Letter stated that Plaintiffs' PII may have been compromised, and included the following:

> **What Happened?** On January 21, 2021, we discovered suspicious activity in our network environment. We immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity and contacted the FBI. Our investigation determined that an unauthorized actor entered our environment between January 21 and 23, 2021, accessed certain files, and took a limited number of files. Therefore, we conducted an extensive review process to analyze the contents of the files potentially accessed to determine what, if any, sensitive information was contained within them. On May 4, 2021 and in the weeks following, we determined that the potentially accessed files contained sensitive information of certain individuals, including you. However, we do not currently have evidence that the files containing your personal information were actually taken by the unauthorized actor. Our investigation remains ongoing, but we wanted to notify you as soon as possible.
>
> **What information Was Involved?** We determined that the following information related to you may have been present in the files that were potentially accessed by the unauthorized actor: name, Social Security number or National ID, date of birth, and driver's license number.

[4] https://careers.wm.com/internal/moreinfo/Life-at-WM-internal, last visited June 14, 2021.

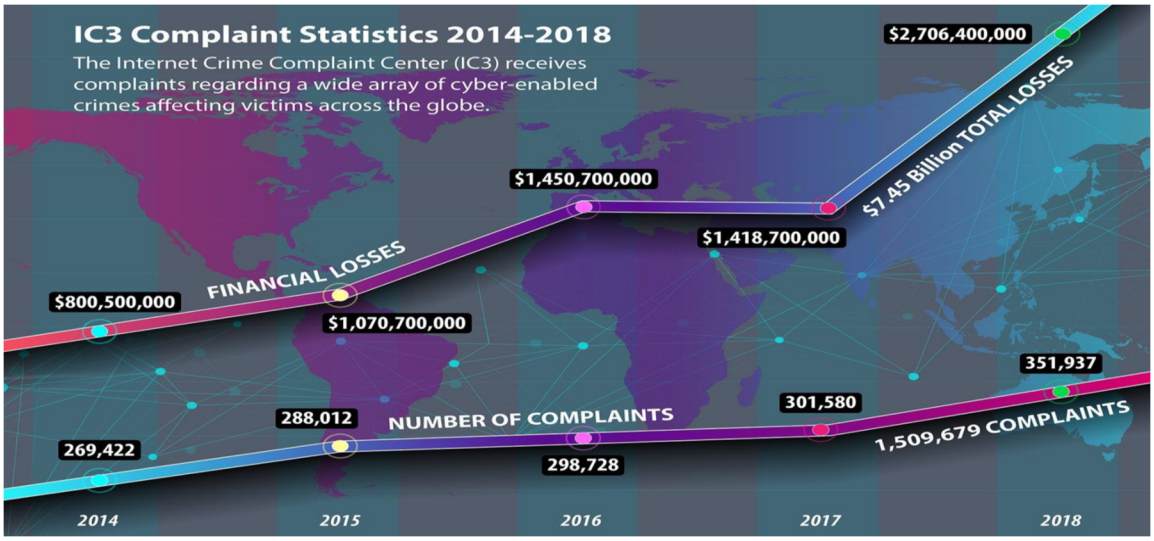
> **What We Are Doing.** We take the confidentiality, privacy, and security of information in in our care seriously. Upon discovery, we immediately commenced an investigation to confirm the nature and scope of the incident. While the investigation remains ongoing, we are taking steps now to implement additional safeguards and review policies and procedures relating to data privacy and security.[5]

18. After receiving the Notice Letter, it is reasonable for recipients, including Plaintiffs and Class members, to believe that the risk of future harm (including identity theft) is substantial and imminent, and to take steps to mitigate that substantial risk of future harm. In fact, in the Notice Letter, WM warns affected individuals of the "incident that may affect some of your information" and provides "steps you may take to better protect against possible misuse of your personal information." *See* **Exs. A & B**.

C. The PII exposed by WM as a result of its inadequate data security is highly valuable on the black market.

19. The information exposed by WM is a virtual goldmine for phishers, hackers, identity thieves and cyber criminals.

20. This exposure is tremendously problematic. Cybercrime is rising at an alarming rate, as shown in the FBI's Internet Crime Complaint statistics chart shown below:



[5] *See* Exs. A & B.

21. By 2013, it was being reported that nearly one out of four data breach notification recipients becomes a victim of identity fraud.[6]

22. Stolen PII is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

23. When malicious actors infiltrate companies and copy and exfiltrate the PII that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[7]

24. For example, when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[8]

---

[6] Pascual, Al, "2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters," *Javelin* (Feb. 20, 2013).

[7] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce, Dec. 28, 2020, *available at:* https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited June 1, 2021).

[8] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, *available at:* https://www.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-

25. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. 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.[9] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[10] Criminals can also purchase access to entire company data breaches for $900 to $4,500.[11]

26. Social Security numbers, for example, 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 illegally using your Social Security number and assuming your identity can cause a lot of problems.[12]

27. What is more, it is no easy task to change or cancel a stolen Social Security number.

---

dark-web/ (last visited June 1, 2021).

[9] *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 visited June 1, 2021).

[10] *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 June 1, 2021).

[11] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited June 1, 2021).

[12] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited June 1, 2021).

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.

28. 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."[13]

29. Because of this, the information compromised in the Data Breach here 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.

30. The PII compromised in the Data Breach 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 10 times on the black market."[14]

31. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to

[13] 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 visited June 1, 2021).

[14] 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 visited June 1, 2021).

additional PII being harvested from the victim, as well as PII from family, friends and colleagues of the original victim.

32. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[15]

33. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

34. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

35. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[16] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs

[15] FBI, *2019 Internet Crime Report Released, Data Reflects an Evolving Threat and the Importance of Reporting* (Feb. 11, 2020), *available at*: https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last visited June 20, 2021).

[16] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited June 1, 2021).

and inconveniences repairing damage to their credit records . . . [and their] good name."[17]

D. WM Failed to Comply with Federal Trade Commission Requirements.

36. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[18]

37. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[19] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[20]

38. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security;

---

[17] *Id.*

[18] *See* Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited June 1, 2021).

[19] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), *available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 1, 2021).

[20] *Id.*

monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[21]

39. Highlighting the importance of protecting against phishing and other types of data breaches, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[22]

40. By being negligent in securing Plaintiffs' and Class members' PII and allowing an unauthorized actor to access WM's network environment, WM failed to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee data. WM's data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

E. Plaintiff Marcaurel's Experience

41. Plaintiff Marcaurel was employed by Waste Management, Inc. at its Modesto Transfer Station located at 2769 W Hatch Rd, Modesto, California in or about 1998 through 1999 handling payroll in the customer service department.

42. A few days after May 28, 2021 Plaintiff Marcaurel received the Notice Letter from WM informing her of the Data Breach.

---

[21] Federal Trade Commission, *Start With Security*, *supra*, footnote 19.
[22] Federal Trade Commission, *Privacy and Security Enforcement Press Releases*, *available at*: https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited June 1, 2021).

43. After receiving notification of the Data Breach, Plaintiff Marcaurel noticed an uptick in the amount and frequency of phishing emails she was receiving, specifically including unwanted information regarding car warranties.

44. Plaintiff Marcaurel has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone and sorting through her unsolicited emails, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This is time that has been lost forever and cannot be recaptured.

45. Plaintiff Marcaurel is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

46. Plaintiff Marcaurel stores all documents containing her PII in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for the few online accounts that he has.

47. Plaintiff Marcaurel has suffered actual injury in the form of damages to, and diminution in, the value of her PII – a form of intangible property that Plaintiff Marcaurel entrusted to Defendants for the purpose of her employment well over 20 years ago. This PII was compromised in, and has been diminished as a result of, the Data Breach.

48. Plaintiff Marcaurel has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

49. Plaintiff Marcaurel has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII resulting from the

compromise of her PII, especially her Social Security number, in combination with her full name and driver's license number, which PII is now in the hands of cyber criminals and other unauthorized third parties.

50. Knowing that thieves stole her PII, including her Social Security number, driver's license number and other PII that she was required to provide to WM, and knowing that her PII will be sold on the dark web, has caused Plaintiff Marcaurel great anxiety.

51. Additionally, Plaintiff Marcaurel is not aware of having been involved in any other data breaches and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. She deletes any and all electronic documents containing her PII and destroys any documents that may contain any of her PII, or that may contain any information that could otherwise be used to compromise her PII.

52. Plaintiff Marcaurel has a continuing interest in ensuring that her PII which, upon information and belief, remains in the possession of Defendants, is protected and safeguarded from future data breaches.

53. As a result of the Data Breach, Plaintiff Marcaurel will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

F. Plaintiff Ingram's Experience

54. Plaintiff Shelby Ingram was employed by Waste Management Natural Services, an affiliate of Defendant WMI, at 2625 West Grandview Road in Phoenix, Arizona from June 29, 2015 through January 19, 2021.

55. A few days after May 28, 2021 Plaintiff Ingram received the Notice Letter from WM informing her of the Data Breach.

56. After receiving notification of the Data Breach, Plaintiff Ingram noticed an uptick in the amount and frequency of phishing emails she was receiving.

57. As a result of the Data Breach, Plaintiff Ingram has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone and sorting through her unsolicited emails, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This is time that has been lost forever and cannot be recaptured.

58. Plaintiff Ingram is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

59. Plaintiff Ingram stores all documents containing her PII in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for the few online accounts that he has.

60. Plaintiff Ingram has suffered actual injury in the form of damages to, and diminution in, the value of her PII – a form of intangible property that Plaintiff Ingram entrusted to Defendant for the purpose of her employment. This PII was compromised in, and has been diminished as a result of, the Data Breach.

61. Plaintiff Ingram has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

62. Plaintiff Ingram has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII resulting from the compromise of her PII, especially her Social Security number, in combination with her full name and driver's license number, which PII is now in the hands of cyber criminals and other unauthorized third parties.

63. Knowing that thieves stole her PII, including her Social Security Number, driver's license number and other PII that she was required to provide to WM, and knowing that her PII will be sold on the dark web, has caused Plaintiff Ingram great anxiety.

64. Additionally, Plaintiff Ingram deletes any and all electronic documents containing her PII and destroys any documents that may contain any of her PII, or that may contain any information that could otherwise be used to compromise her PII.

65. Plaintiff Ingram has a continuing interest in ensuring that her PII which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

66. As a result of the Data Breach, Plaintiff Ingram will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

G. Plaintiffs and the Class members suffered damages.

67. The ramifications of Defendants' failure to keep current and former employees' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.[23]

[23] *2014 LexisNexis True Cost of Fraud Study, available at:* https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last visited June 1, 2021).

68. The PII belonging to Plaintiffs and Class members is private, sensitive in nature, and was left inadequately protected by Defendants who did not obtain Plaintiffs' or Class members' consent to disclose such PII to any other person as required by applicable law and industry standards.

69. Defendants required Plaintiffs and Class members to provide their PII, including full names, driver's license numbers and Social Security numbers. Implied in these exchanges was a promise by Defendants to ensure that the PII of Plaintiffs and Class members in their possession was only used to provide the agreed-upon compensation and other employment benefits from Defendant.

70. Plaintiffs and Class members therefore did not receive the benefit of the bargain with Defendants, because their providing their PII was in exchange for WM's implied agreement to secure it and keep it safe.

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

72. Defendants had the resources necessary to prevent the Data Breach, but neglected to implement adequate data security measures, despite their obligations to protect current and former employees' (and their dependents') PII, and despite their public statements that WM "value[s] safety" and is one of the "world's most ethical companies."

73. Had Defendants remedied the deficiencies in their data security training and

protocols, and adopted security measures recommended by experts in the field, they would have prevented the intrusion leading to the theft of PII.

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

75. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[24]

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

a. The compromise, publication, theft, and/or unauthorized use of their PII;

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

[24] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited June 1, 2021).

d. The continued risk to their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect the PII in their possession; and

e. Current and future costs in terms of time, effort, and money that Plaintiffs will expend to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of Plaintiffs' and Class members' lives.

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

78. To date, other than providing a woefully inadequate twelve (12) months of credit monitoring and identity protection services, Defendants do not appear to be taking any measures to assist Plaintiffs and Class members other than simply telling them to review their financial records and credit reports on a regular basis. This is wildly inadequate especially in light of the fact that some Plaintiffs and Class members worked at WM well over 20 years ago. It begs the question: Why would WM not secure such important and sensitive PII?

79. Defendants' failure to adequately protect Plaintiffs' and Class members' PII has resulted in Plaintiffs and Class members having to undertake tasks requiring extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money – while Defendants sit by and do nothing to assist those affected by the Data Breach. Instead, as Defendants' Notice Letter indicates, they are putting the burden on Plaintiffs and Class members to discover possible fraudulent activity and identity theft.

80. Defendants' offer of 12 months of identity monitoring and identity protection services to Plaintiffs and Class members is woefully inadequate. While some harm has begun

already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is acquired and when it is used. Furthermore, identity theft monitoring services only alert someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's PII) – they do not prevent identity theft.[25] Although their PII was improperly exposed in or about January 2021, affected current and former employees were not notified of the Data Breach until four months later, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach. As a result of WM's delay in detecting and notifying current and former employees of the Data Breach, the risk of fraud for Plaintiffs and Class members has been driven even higher.

CLASS ACTION ALLEGATIONS

81. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action on behalf of themselves and the following proposed Class, defined as follows:

> All persons residing in the United States who are current or former employees of USA Waste-Management Resources, LLC or Waste Management, Inc. or any of their affiliates and had their PII compromised as a result of the Data Breach that occurred between January 21 and 23, 2021 (the "Nationwide Class").

82. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Marcaurel asserts claims on behalf of a separate statewide subclass, defined as follows:

> All individuals residing in California who are current or former employees of USA Waste-Management Resources, LLC or Waste Management, Inc. or any of their affiliates and had their PII compromised as a result of the Data Breach that occurred between January 21 and 23, 2021 (the "California Class").

[25] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, *available at*: https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (last visited June 1, 2021).

83. The "Nationwide Class" and the "California Class" are collectively referred to herein as the "Class."

84. Excluded from the proposed Class are any officer or director of Defendants; any officer or director of any affiliate, parent, or subsidiary of WMI and WMR; and any judge to whom this case is assigned, his or her spouse, and members of the judge's staff.

85. **Numerosity.** Members of the proposed Class likely number in the tens of thousands and are thus too numerous to practically join in a single action. Defendants have reported that 268,510 persons have been affected by the Data Breach.[26] Membership in the Class is readily ascertainable from Defendants' own records.

86. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class members and predominate over questions affecting only individual Class members. These common questions include:

a. Whether Defendants engaged in the wrongful conduct alleged herein;

b. Whether Defendants' inadequate data security measures were a cause of the Data Breach;

c. Whether Defendants owed a legal duty to Plaintiffs and the other Class members to exercise due care in collecting, storing, and safeguarding their PII;

[26] *See, e.g.*, https://apps.web.maine.gov/online/aeviewer/ME/40/e568516f-7c0d-4739-982c-23ff1c094036.shtml (last visited June 20, 2021).

d. Whether Defendants negligently or recklessly breached legal duties owed to Plaintiffs and the Class members to exercise due care in collecting, storing, and safeguarding their PII;

e. Whether Plaintiffs and the Class are at an increased risk for identity theft because of the Data Breach;

f. Whether Defendants failed to implement and maintain reasonable security procedures and practices for Plaintiffs' and Class members' PII in violation Section 5 of the FTC Act;

g. Whether Plaintiffs and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

h. Whether Plaintiffs and the other Class members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

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

88. **Typicality.** Plaintiffs' claims are typical of the claims of the members of the Class. All Class members were subject to the Data Breach and had their PII accessed by and/or disclosed to unauthorized third parties. Defendants' misconduct impacted all Class members in the same manner.

89. **Adequacy of Representation.** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class members they seek to

represent; they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

90. **Superiority.** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class members to individually seek redress for Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION
Negligence
(On behalf of Plaintiffs and the Class)

91. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

92. Defendants owed a duty to Plaintiffs and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class members' PII from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, maintaining, and testing its data security systems to ensure that Plaintiffs' and Class members' PII in Defendants' possession was adequately secured and protected.

93. Defendants owed a duty of care to Plaintiffs and members of the Class to provide

security, consistent with industry standards, to ensure that its protocols, systems, and networks adequately protected the PII of its current and former employees.

94. Defendants owed a duty of care to Plaintiffs and Class members because they were foreseeable and probable victims of any inadequate data security practices. Defendants knew or should have known of the inherent risks in collecting and storing the PII of its current and former employees (and their dependents) and the critical importance of adequately securing such information.

95. Plaintiffs and Class members entrusted Defendants with their PII with the understanding that Defendants would safeguard it, that Defendants would not store it longer than necessary, and that Defendants were in a position to protect against the harm suffered by Plaintiffs and Class members as a result of the Data Breach.

96. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their PII. Defendants' misconduct included failing to implement the necessary systems, policies, employee training and procedures necessary to prevent the Data Breach.

97. Defendants knew, or should have known, of the risks inherent in collecting and storing PII and the importance of adequate security. Defendants knew about – or should have been aware of – numerous, well-publicized data breaches affecting businesses in the United States.

98. Defendants breached their duties to Plaintiffs and Class members by failing to provide fair, reasonable, or adequate computer systems and data security to safeguard the PII of Plaintiffs and Class members.

99. Plaintiffs' injuries and damages, as described below, are a reasonably certain consequence of Defendants' breach of their duties.

100. Because Defendants knew that a breach of their systems would damage thousands

of current and former WM employees, Defendants had a duty to adequately protect their data systems and the PII contained therein.

101. Defendants had a special relationship with current and former employees, including with Plaintiffs and Class members, by virtue of their being current or former employees. Plaintiffs and Class members reasonably believed that Defendants would take adequate security precautions to protect their PII. Defendants also had independent duties under state and federal laws that required Defendants to reasonably safeguard Plaintiffs' and Class members' PII.

102. Through Defendants' acts and omissions, including Defendants' failure to provide adequate security and its failure to protect Plaintiffs' and Class members' PII from being foreseeably accessed, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure the PII of Plaintiffs and Class members during the time it was within their possession or control.

103. In engaging in the negligent acts and omissions as alleged herein, which permitted an "unauthorized actor" to access the WM network environment, Defendants failed to meet the data security standards set forth under Section 5 of the FTC Act, which prohibits "unfair … practices in or affecting commerce." This prohibition includes failing to have adequate data security measures, which Defendants have failed to do as discussed herein.

104. Defendants' failure to meet this standard of data security established under Section 5 of the FTC Act is evidence of negligence.

105. Neither Plaintiffs nor the other Class members contributed to the Data Breach as described in this Complaint.

106. As a direct and proximate cause of Defendants' actions and inactions, including but not limited to their failure to properly encrypt their systems and otherwise implement and maintain

reasonable security procedures and practices, Plaintiffs and Class members have suffered and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PII is used; (ii) the publication and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protection; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of employees and former employees in their continued possession; and (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On behalf of Plaintiffs and the Class)

107. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

108. Defendants offered employment to the current or former employees, including Plaintiffs and Class members, either directly or through acquiring the businesses for which Plaintiffs and Class members worked, in exchange for compensation and other employment benefits.

109. Defendants required Plaintiffs and Class members to provide their PII, including

names, driver's license number, dates of birth, Social Security numbers (or National IDs) and other personal information. Implied in these exchanges was a promise by Defendants to ensure that the PII of Plaintiffs and Class members in their possession was only used to provide the agreed-upon compensation and other employment benefits.

110. These exchanges constituted an agreement between the parties: Plaintiffs and Class members would provide their PII in exchange for the prospect of employment and benefits provided by Defendants.

111. These agreements were made either by Plaintiffs or Class members applying for employment with Defendants, being employed by Defendants, or their employers being acquired by Defendants.

112. It is clear by these exchanges that the parties intended to enter into an agreement. Plaintiffs and Class members would not have disclosed their PII to Defendants but for the prospect of Defendants' promise of compensation and other employment benefits. Conversely, Defendants presumably would not have taken Plaintiffs' and Class members' PII if they did not intend to provide Plaintiffs and Class members compensation and other employment benefits, or, in the case of applicants, consider hiring them.

113. Defendants was therefore required to reasonably safeguard and protect the PII of Plaintiffs and Class members from unauthorized disclosure and/or use.

114. Plaintiffs and Class members accepted Defendants' employment offer and fully performed their obligations under the implied contract with Defendants by providing their PII, directly or indirectly, to Defendants, among other obligations.

115. Plaintiffs and Class members would not have provided and entrusted their PII to Defendants in the absence of their implied contracts with Defendants and would have instead retained the opportunity to control their PII for uses other than compensation and other employment benefits from Defendants.

116. Defendants breached the implied contracts with Plaintiffs and Class members by failing to reasonably safeguard and protect Plaintiffs' and Class members' PII.

117. Defendants' failure to implement adequate measures to protect the PII of Plaintiffs and Class members violated the purpose of the agreement between the parties: Plaintiffs' and Class members' employment in exchange for compensation and benefits.

118. Defendants were on notice that their systems and data security protocols could be inadequate yet failed to invest in the proper safeguarding of Plaintiffs' and Class members' PII.

119. Instead of spending adequate financial resources to safeguard Plaintiffs' and Class members' PII, which Plaintiffs and Class members were required to provide to Defendants, Defendants instead used that money for other purposes, thereby breaching their implied contracts it had with Plaintiffs and Class members.

120. As a proximate and direct result of Defendants' breaches of its implied contracts with Plaintiffs and Class members, Plaintiffs and the Class members suffered damages as described in detail above.

THIRD CAUSE OF ACTION
Breach of Confidence
(On behalf of Plaintiffs and the Class)

121. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

122. At all times during Plaintiffs' and Class members' interactions with Defendants as their employees, Defendants were fully aware of the confidential and sensitive nature of Plaintiffs'

and Class members' PII that Plaintiffs and Class members provided to Defendants.

123. Plaintiffs' and Class members' PII constitutes confidential and novel information. Indeed, Plaintiffs' and Class members' Social Security numbers can be changed only with great difficulty and time spent, which still enables a threat actor to exploit that information during the interim; additionally, 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.

124. As alleged herein and above, Defendants' relationship with Plaintiffs and Class members was governed by terms and expectations that Plaintiffs' and Class members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

125. Plaintiffs and Class members provided their respective PII to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the PII to be disseminated to any unauthorized parties.

126. Defendants voluntarily received in confidence Plaintiffs' and Class members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

127. Due to Defendants' failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, following best information security practices and providing proper employee training to secure Plaintiffs' and Class members' PII, Plaintiffs' and Class members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class

members' confidence, and without their express permission.

128. As a direct and proximate cause of Defendants' actions and/or omissions, Plaintiffs and Class members have suffered damages.

129. But for Defendants' disclosure of Plaintiffs' and Class members' PII, in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants' Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class members' PII, as well as the resulting damages.

130. This disclosure of Plaintiffs' and Class members' PII constituted a violation of Plaintiffs' and Class members' understanding that Defendants would safeguard and protect the confidential and novel PII that Plaintiffs and Class members were required to disclose to Defendants.

131. The injury and harm Plaintiffs and Class members suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiffs' and Class members' PII. Defendants knew their data security procedures for accepting and securing Plaintiffs' and Class members' PII had numerous security and other vulnerabilities that placed Plaintiffs' and Class members' PII in jeopardy.

132. As a direct and proximate result of Defendants' breaches of confidence, Plaintiffs and Class members have suffered and/or are at a substantial risk of suffering injury that includes but is not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) 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; (e) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession; and (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class members.

FOURTH CAUSE OF ACTION
Invasion of Privacy
(On behalf of Plaintiffs and the Class)

133. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

134. Plaintiffs and Class members had a legitimate and reasonable expectation of privacy with respect to their PII and were accordingly entitled to the protection of this personal information against disclosure to and acquisition by unauthorized third parties.

135. Defendants owed a duty to their employees, including Plaintiffs and Class members, to keep their PII confidential.

136. The unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of PII, especially the PII that is the subject of this action, is highly offensive to a reasonable person.

137. The intrusion was into a place or thing that was private and is entitled to remain private. Plaintiffs and Class members disclosed their PII to Defendants as part of their employment with Defendants, but did so privately with the intention and understanding that the PII would be kept confidential and protected from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing. Plaintiffs and Class members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization. The Data Breach, which was caused by Defendants' negligent actions and inactions, constitutes an intentional interference with Plaintiffs' and Class members' interest

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

138. Defendants acted with a knowing state of mind when they permitted the Data Breach because they knew their information security practices were inadequate.

139. Defendants invaded Plaintiffs' and Class members' privacy by failing to adequately implement data security measures, despite their obligations to protect current and former employees' highly sensitive PII.

140. Defendants' motives leading to the Data Breach were financially based. In order to save on operating costs, Defendants decided against the implement of adequate data security measures.

141. Defendants' intrusion upon Plaintiffs' and Class members' privacy in order to save money constitutes an egregious breach of social norms.

142. Acting with knowledge, Defendants had notice and knew that their inadequate cybersecurity practices would cause injury to Plaintiffs and Class members.

143. As a proximate result of Defendants' acts and omissions, Plaintiffs' and Class members' PII was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, obtained by, released to, stolen by, used by, and/or viewed by third parties without authorization, causing Plaintiffs and Class members to suffer damages.

144. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class members in that the PII maintained by Defendants can still be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized persons.

145. Plaintiffs and Class members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class members.

FIFTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On behalf of Plaintiffs and the Class)

146. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

147. In light of their special relationship, Defendants became the guardian of Plaintiffs' and Class members' PII. Defendants became fiduciaries, created by their undertaking and guardianship of their employees' PII, to act primarily for the benefit of those employees, including Plaintiffs and Class members. This duty included the obligation to safeguard Plaintiffs' and Class members' PII and to timely detect and notify them in the event of a data breach.

148. In order to provide Plaintiffs and Class members compensation and employment benefits, or to consider Plaintiffs and Class members for employment, Defendants required that Plaintiffs and Class members provide their PII.

149. Defendants knowingly undertook the responsibility and duties related to the possession of Plaintiffs' and Class members' PII for the benefit of Plaintiffs and Class members in order to provide Plaintiffs and Class members compensation and employment benefits.

150. Defendants have a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of their relationship with them. Defendants breached their fiduciary duties owed to Plaintiffs and Class members by failing to properly encrypt and otherwise protect Plaintiffs' and Class members' PII. Defendants further breached their fiduciary duties owed to Plaintiffs and Class members by failing to timely detect the Data Breach and notify and/or warn Plaintiffs and Class members of the Data Breach.

151. As a direct and proximate result of Defendants' breaches of their fiduciary duties,

Plaintiffs and Class members have suffered or will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their PII is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (e) lost opportunity costs associated with efforts 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; (f) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' PII in its continued possession; and (g) 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 Plaintiffs' and Class members' lives.

152. As a direct and proximate result of Defendants' breach of their fiduciary duty, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

SIXTH CAUSE OF ACTION
Violation of California's Consumer Privacy Act
Cal. Civ. Code § 1798.150
(On behalf of Plaintiff Marcaurel and the California Class)

153. Plaintiff Janie Marcaurel incorporates the foregoing paragraphs as though fully set forth herein.

154. Defendants violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiff Marcaurel's and California Class members' PII from

unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff Marcaurel and California Class members.

155. As a direct and proximate result of Defendants' acts, Plaintiff Marcaurel's and the California Class members' PII was subjected to unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violation of the duty.

156. As a direct and proximate result of Defendants' acts, Plaintiff Marcaurel and the California Class members were injured and lost money or property, including but not limited the loss of California Class members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

157. Defendants knew or should have known that their network computer systems and data security practices were inadequate to safeguard Plaintiff Marcaurel's and California Class members' PII and that the risk of a data breach or theft was highly likely. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff Marcaurel and the California Class members.

158. Defendants are organized for the profit or financial benefit of their owners and collects PII as defined in Cal. Civ. Code § 1798.140.

159. Plaintiff Marcaurel and the California Class members seek injunctive or other equitable relief to ensure Defendants hereinafter adequately safeguard Plaintiff Marcaurel's and the California Class members' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendants continue to hold Plaintiff Marcaurel's and the California Class members' PII. These individuals have an interest in ensuring that their PII is

reasonably protected.

160. On June 21, 2021, Plaintiff Marcaurel's counsel sent a notice letter to Defendants' registered service agents via certified mail. Assuming Defendants do not cure the Data Breach within 30 days, and Plaintiff Marcaurel believes any such cure is not possible under these facts and circumstances, Plaintiff Marcaurel intends to promptly amend this Complaint to seek actual damages and statutory damages of no less than $100 and up to $750 per customer record subject to the Data Breach on behalf of the California Class as authorized by the CCPA.

SEVENTH CAUSE OF ACTION
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq*.
(On behalf of Plaintiff Marcaurel and the California Class)

161. Plaintiff Janie Marcaurel incorporates the foregoing paragraphs as though fully set forth herein.

162. By reason of the conduct alleged herein, Defendants engaged in unlawful and unfair business practices within the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200, *et seq*.

163. Defendants stored the PII of Plaintiff Marcaurel and the California Class members in their network environment. Defendants falsely represented to Plaintiff Marcaurel and the California Class members that their PII was secure and would remain private or, alternatively, failed to disclose to Plaintiff Marcaurel and the California Class members that their PII was not secure.

164. Defendants knew or should have known they did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations and that would have kept Plaintiff Marcaurel's and the California Class members' PII secure and prevented the loss or misuse of that PII.

165. Even without these misrepresentations and omissions, Plaintiff Marcaurel and the California Class members were entitled to assume, and did assume, that Defendants would take appropriate measures to keep their PII safe. Defendants did not disclose at any time that Plaintiff Marcaurel's and the California Class members' PII was vulnerable to hackers because Defendants' data security measures were inadequate and most likely outdated, and Defendants were the only ones in possession of that material information, which they had a duty to disclose.

Unlawful Business Practices

166. Defendants violated Section 5(a) of the FTC Act (which is a predicate legal violation for this UCL claim) by misrepresenting, both by affirmative conduct and by omission, the safety of their network environment, specifically the security thereof, and their ability to safely store Plaintiff Marcaurel's and the California Class members' PII.

167. Defendants also violated Section 5(a) of the FTC Act by failing to implement reasonable and appropriate security measures or follow industry standards for data security, and by failing to timely notify Plaintiff Marcaurel and the California Class members of the Data Breach.

168. Defendants also violated California Civil Code § 1798.81.5(b) in that they failed to maintain reasonable security procedures and practices.

169. If Defendants had complied with these legal requirements, Plaintiff Marcaurel and the California Class members would not have suffered the damages related to the Data Breach, and from Defendants' failure to timely notify Plaintiff Marcaurel and the California Class members of the Data Breach.

170. Defendants' acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Section 5(a) of the FTC Act.

171. Plaintiff Marcaurel and the California Class members suffered injury in fact and lost money or property as the result of Defendants' unlawful business practices. In addition, Plaintiff Marcaurel's and the California Class members' PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff Marcaurel and the California Class members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

Unfair Business Practices

172. Defendants engaged in unfair business practices under the "balancing test." The harm caused by Defendants' actions and omissions greatly outweigh any perceived utility. Indeed, Defendants' failure to follow basic data security protocols and misrepresentations to current and former employees about Defendants' data security cannot be said to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiff Marcaurel and the California Class members, directly causing the harms.

173. Defendants also engaged in unfair business practices under the "tethering test." Defendants' actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. *See*, *e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the

Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendants' acts and omissions thus amount to a violation of the law.

174. Defendants engaged in unfair business practices under the "FTC test." The harm caused by Defendants' actions and omissions, as described in detail above, is substantial in that it affects thousands of California Class Members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Plaintiff Marcaurel's and the California Class members' PII to third parties without their consent, diminution in value of their PII, consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. This harm continues given the fact that Plaintiff Marcaurel's and the California Class members' PII remains in Defendants' possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendant's actions and omissions violated Section 5(a) of the Federal Trade Commission Act. *See* 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"); *see also*, *e.g.*, *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act).

175. Plaintiff Marcaurel and the California Class members suffered injury in fact and lost money or property as the result of Defendants' unfair business practices. Plaintiff Marcaurel's and the California Class members' PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff Marcaurel and the California Class members have also suffered

consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

176. As a result of Defendants' unlawful and unfair business practices in violation of the UCL, Plaintiff Marcaurel and the California Class members are entitled to damages, injunctive relief, and reasonable attorneys' fees and costs.

EIGHTH CAUSE OF ACTION
Violation of California's Customer Records Act
Cal. Civ. Code § 1798.80, *et seq*.
(On behalf of Plaintiff Marcaurel and the California Class)

177. Plaintiff Marcaurel incorporates the foregoing paragraphs as though fully set forth herein.

178. Section 1798.82 of the California Civil Code, part of the California Customer Records Act ("CCRA"), requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay . . . ."

179. The CCRA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b).

180. Any person or business that is required to issue a security breach notification under the CCRA shall meet all of the following requirements:

1. The security breach notification shall be written in plain language,
2. The security breach notification shall include, at a minimum, the following information:
    a) The name and contact information of the reporting person or business subject to this section,
    b) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach,
    c) If the information is possible to determine at the time the notice is provided, then any of the following:
        i. The date of the breach,
        ii. The estimated date of the breach, or
        iii. The date range within which the breach occurred. The notification shall also include the date of the notice,
        iv. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided,
        v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided, and
        vi. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

181. As alleged above, Defendants unreasonably delayed (not less than 65 days) informing Plaintiff Marcaurel and the California Class members about the Data Breach, affecting their PII, after Defendants knew the Data Breach had occurred.

182. Defendants failed to disclose to Plaintiff Marcaurel and the California Class members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, PII when Defendants knew or reasonably believed such information had been compromised.

183. Defendants' ongoing business interests gave Defendants incentive to conceal the Data Breach from the public to ensure continued revenue.

184. Upon information and belief, no law enforcement agency instructed Defendants that timely notification to Plaintiff Marcaurel and the California Class members would impede its investigation.

185. As a result of Defendants' violation of Cal. Civ. Code § 1798.82, Plaintiff Marcaurel and the California Class members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff Marcaurel and the California Class members because their stolen information would have had less value to identity thieves.

186. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff Marcaurel and the California Class members incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

187. Plaintiff Marcaurel and the California Class members seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to the damages suffered by Plaintiff

Marcaurel and the California Class members as alleged above and equitable relief.

NINTH CAUSE OF ACTION
Declaratory and Injunctive Relief
(On behalf of Plaintiffs and Nationwide Class)

188. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

189. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. § 2201.

190. As previously alleged, Plaintiffs and Class members entered into an implied contract that required Defendants to provide adequate security for the PII it collected from Plaintiffs and Class members.

191. Defendants owe a duty of care to Plaintiffs and Class members requiring them to adequately secure their PII.

192. Defendants still possess PII regarding Plaintiffs and Class members.

193. Since the Data Breach, Defendants have announced few if any changes to their data security infrastructure, processes, or procedures to fix the vulnerabilities in their computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent future attacks.

194. Defendants have not satisfied their contractual obligations and legal duties to Plaintiffs and Class members. In fact, now that Defendants' insufficient data security is known to hackers, the PII in Defendants' possession is even more vulnerable to cyberattack.

195. Actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide security measures to Plaintiffs and Class members. Further, Plaintiffs and Class members are at risk of additional or further harm due to the exposure of their PII and Defendants' failure to address the security failings that led to such

exposure.

196. There is no reason to believe that Defendants' security measures are any more adequate now than they were before the Data Breach to meet Defendants' contractual obligations and legal duties.

197. Plaintiffs, therefore, seek a declaration (1) that Defendants' existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (2) that to comply with their contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

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

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendants segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Ordering that Defendants purge, delete, and destroy in a reasonably secure manner employee data not necessary for their provisions of services;

f. Ordering that Defendants conduct regular computer system scanning and security checks;

g. Ordering that Defendants routinely and continually conduct 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; and

h. Ordering Defendants to meaningfully educate their current, former, and prospective employees about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of themselves and all others similarly situated, respectfully requests that the Court enter an order:

a. Certifying the proposed Classes as requested herein;

b. Appointing Plaintiffs as Class Representatives and the undersigned counsel as Class Counsel;

c. Finding that Defendants engaged in the unlawful conduct as alleged herein;

d. Granting injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class members, including but not limited to an order:

i. Prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. Requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the PII of Plaintiffs and Class members unless WM can provide to the Court reasonable justification for the

retention and use of such information when weighed against the privacy interests of Plaintiffs and Class members;

iv. requiring Defendants to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of Plaintiffs' and Class members' PII;

v. prohibiting Defendants from maintaining Plaintiffs' and Class members' PII on a cloud-based database;

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

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of their network is compromised, hackers cannot gain access to other portions of their systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with

additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiffs and Class members,

xii. requiring Defendants to conduct internal training and education routinely and continually and, on an annual basis, inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting PII;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to design, maintain, and test their computer systems to ensure that PII in their possession is adequately secured and protected;

xvii. requiring Defendants to detect and disclose any future data breaches in a timely

and accurate manner;

xviii. requiring Defendants to implement multi-factor authentication requirements, if not already implemented;

xix. requiring Defendants' employees to change their passwords on a timely and regular basis, consistent with best practices; and

xx. requiring Defendants to provide lifetime credit monitoring and identity theft repair services to Class members.

e. Awarding Plaintiffs and Class members damages;

f. Awarding Plaintiffs and Class members pre-judgment and post-judgment interest on all amounts awarded;

g. Awarding Plaintiffs and the Class members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the proposed Class, hereby demand a trial by jury as to all matters so triable.

Date: June 21, 2021

Respectfully Submitted,

/s/ Joe Kendall

Joe Kendall
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Ste. 1450
Dallas, TX 75219
Telephone: 214/744-3000
Facsimile: 214/744-3015
jkendall@kendalllawgroup.com

M. Anderson Berry
(Pro Hac Vice application forthcoming)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com

Rachele R. Byrd
byrd@whafh.com
Brittany N. DeJong
dejong@whafh.com
WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, California
Telephone: (619) 239-4599
Facsimile: (619) 234-4599

Attorneys for Plaintiffs and the Class

ClassAction.org
