UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN RE: WASTE MANAGEMENT DATA BREACH LITIGATION	No. 21-cv-6199-DLC **AMENDED CONSOLIDATED CLASS ACTION COMPLAINT**

Plaintiffs Janie Marcaurel ("Marcaurel"), Gabriel Fierro ("Fierro"), Shelby Ingram ("Ingram"), Mark Krenzer ("Krenzer"), Mary J. Fusilier ("Fusilier"), Clifford Harris ("Harris"), Nolan Brodie ("Brodie"), Miguel Montelongo ("Montelongo"), Gerald Davis ("Davis"), and Steven Dudley ("Dudley") individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to them and on information and belief as to all other matters, by and through undersigned counsel, hereby bring this Consolidated Class Action Complaint against USA Waste-Management Resources, LLC ("Defendant" or "Waste Management"), and allege as follows:

INTRODUCTION

1. In a recent Executive Order, President Joe Biden reaffirmed that "[t]he United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy."[1] Among other things, the Order noted "[t]he private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (last visited Nov. 19, 2021).

infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced."[2]

2. Here, unfortunately, Defendant, as Plaintiffs' and the putative Class's current or former employer, violated that trust, leaving Plaintiffs and the putative Class to incur the consequences. According to Defendant's notice filed with the Office of the Maine Attorney General, computer hackers stole from Defendants the sensitive personal identifying information of 268,510 of Defendant's employees, former employees and their dependents.[3]

3. Businesses, such as Defendant, that collect and store sensitive information about their employees and employees' families have statutory, regulatory, contractual, and common law duties to safeguard that information and ensure it remains private. These duties are essential where an employer keeps and stores its current and former employees' highly personal information such as their names, Social Security numbers, dates of birth, national IDs, health information, and driver's license numbers.

4. Here, Defendant is the largest waste management company in the United States, providing solid waste and recycling services to millions of residential, commercial, industrial, and municipal customers. Defendant had numerous statutory, regulatory, contractual, and common law obligations to keep Plaintiffs' and the Class Members' personally identifiable information confidential, safe, secure, and protected from unauthorized disclosure or access.

5. Defendant's job applicants and employees are required to provide valuable personal identifying information to their employer, including Social Security numbers, driver's license numbers, dates of birth and addresses in order to obtain employment. Defendant was and still is

[2] *Id.*

[3] **Exhibit A,** Office of the Maine Attorney General, *Data Breach Notifications*.

obligated to secure that personal identifying information by implementing reasonable and appropriate data security safeguards.

6. Plaintiffs bring this action against Defendant for its failure to properly secure and safeguard personally identifiable information Defendant required from its employees as a condition of employment, including their full names, Social Security numbers (or National IDs), dates of birth, and driver's license numbers (collectively, "PII").[4]

7. Plaintiffs also allege Defendant failed to provide timely notice to Plaintiffs and current and former employees and their dependents (collectively, "Class members") that their PII had been lost and precisely what types of information were unencrypted and in the possession of unknown and unauthorized third parties.[5]

8. Defendant makes several claims that it acknowledges and complies with privacy and data protection laws. For example, in its Code of Conduct, Defendant promises:

> We respect the privacy of our customers, co-workers and business partners. We handle personally identifiable information and other information with proper care and diligence. We comply with our privacy and other internal policies, contractual obligations and applicable privacy and data protection laws. These laws cover how

[4] 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 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).

[5] The information exposed in the Data Breach was unencrypted. California law requires companies to notify California residents "whose **unencrypted** personal information was, or is reasonably believed to have been, acquired by an unauthorized person" due to a "breach of the security of the system[.]" Cal. Civ. Code § 1798.82(a)(1) (emphasis added). Defendant notified the California Attorney General of the Data Breach on or about May 28, 2021, evidencing that the exposed data was unencrypted. *See* https://oag.ca.gov/ecrime/databreach/reports/sb24-541404 (last visited Nov. 17, 2021).

> to responsibly collect, store, use, share, transfer and dispose of personally identifiable information.[6]

9. Defendant also boasts it "value[s] safety" and is one of the "world's most ethical companies . . . ." [7] Defendant also contractually agreed that employees' personally identifiable information is private and confidential.[8] Defendant has also acknowledged the risks involved in connecting its computer network to the internet as doing so exposes the network to additional risks of unauthorized intrusion.

10. Even knowing in advance about the risks, however, Defendant failed to meet its obligations to properly secure and protect the sensitive PII entrusted to it by its current and former employees.

11. As a result of Defendant's failure to exercise due care, an unauthorized third party (aka a "hacker") accessed, acquired, and stole the sensitive PII from Defendant's system. As reported by Defendant, between January 21 and 23, 2021, an unauthorized actor entered its environment and accessed and took a number of files (the "Data Breach"). On May 4, 2021, and during the weeks following, Defendant determined the Data Breach included files containing 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.

---

[6] Waste Management Code of Conduct, April 2021, *available at*: https://sustainability.wm.com/downloads/WM_Code_of_Conduct.pdf (last visited Nov. 19, 2021).

[7] 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 Nov. 19, 2021).

[8] The agreement states it is not to be reproduced or distributed outside of Waste Management without the company's approval.

12. Defendant did not provide notice to its current and former employees of the data breach until May 28, 2021, when it mailed data breach notices to those individuals whose PII was accessed by unauthorized third parties.

13. As a result of Defendant's failure to provide reasonable and adequate data security, Plaintiffs and the Class members are and will continue to be at a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class members must now and in the future closely monitor their financial accounts to guard against identity theft.

14. Plaintiffs and members of the proposed Class have suffered actual and imminent injuries as a direct result of the data breach. The actual and imminent injuries suffered by Plaintiffs and the proposed Class as a direct result of the data breach include:

a. theft of their personal data;

b. costs associated with the detection and prevention of identity theft;

c. costs associated with time spent and the loss of productivity from taking time to address and attempt to monitor, ameliorate, mitigate and deal with the consequences of the data breach;

d. the stress, nuisance and annoyance of dealing with all issues resulting from the data breach;

e. actual fraudulent activity on financial accounts;

f. increased fraudulent robo calls and spoofing email attempts;

g. the potential for future fraud and the increased risk of identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals;

h. damages to and diminution in value of their personal data entrusted to Defendant;

i. Defendant's retention of the reasonable value of the PII entrusted to it; and

j. the continued risk to their personal data which remains in Defendant's possession, and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its possession.

15. Plaintiffs seek to remedy these injuries and prevent their current and future occurrences on behalf of themselves and all similarly situated individuals whose PII was accessed, compromised and stolen as a result of the Data Breach.

16. Plaintiffs on behalf of themselves and the Nationwide Class and California Class (as defined *infra*) request remedies including damages, reimbursement of out-of-pocket costs, and equitable and injunctive relief, including improvements to Defendant's data security systems, future annual audits, ID protection services funded by Defendant, and statutory damages for the California Subclass.

THE PARTIES

Plaintiffs

17. Plaintiff Marcaurel is a resident and citizen of California, and was employed by Defendant at the Modesto facility in or about 1998 through 1999. Ms. Marcaurel, in connection with her employment, entrusted to Defendant her PII and reasonably believed Defendant would keep her PII secure. Had Defendant disclosed it would not keep her PII secure and 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 Defendant dated May 28, 2021, on or about that date.

18. Plaintiff Fierro is a resident and citizen of California, and is a current employee of USA Waste of California, Inc., an affiliate of Defendant, at its facility located in Chino, California, and has worked for Defendant since August 2019. Mr. Fierro, in connection with his employment, entrusted to Defendant his PII and reasonably believed Defendant would keep his PII secure. Had Defendant disclosed it would not keep his PII secure and that it would be easily accessible to hackers and third parties, he would have taken additional precautions relating to his PII. He received a Notice of Data Breach from Defendant dated May 28, 2021, in or about June 2021.

19. Plaintiff Ingram is a resident and citizen of Arizona, and was employed by Defendant in the Phoenix Call Center from or about June 29, 2005 through January 19, 2020. Ms. Ingram, in connection with her employment, entrusted to Defendant her PII and reasonably believed Defendant would keep her PII secure. Had Defendant disclosed it 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 Defendant dated June 4, 2021, in or around June 2021.

20. Plaintiff Krenzer is a resident and citizen of Texas, and was employed by Defendant at the corporate headquarters in Houston, Texas in or about 2008 through 2014. Mr. Krenzer, in connection with his employment, entrusted to Defendant his PII and reasonably believed Defendant would keep his PII secure. Had Defendant disclosed it would not keep his PII secure and that it would be easily accessible to hackers and third parties, he would have taken additional precautions relating to his PII. He received a Notice of Data Breach from Defendant dated June 4, 2021, on or about that date.

21. Plaintiff Fusilier is a resident and citizen of Texas, and she was employed by Defendant in the sustainability division located in Houston, Texas from 2006 to 2015. Plaintiff Fusilier, in connection with her employment, entrusted her PII to Defendant and reasonably believed Defendant would keep her PII secure. Had Defendant disclosed it would not keep her PII secure and that it would be easily accessible to hackers and third parties, she would have taken additional precautions to protect her PII. Plaintiff Fusilier received a Notice of Data Breach from Defendant dated June 4, 2021, in or around June 2021.

22. Plaintiff Harris is a resident and citizen of Illinois. From 1998 to 2005, he was employed by Defendant as a National Account Executive. Plaintiff Harris, in connection with his employment, entrusted his PII to Defendant and reasonably believed Defendant would keep his PII secure. Had Defendant disclosed it would not keep his PII secure and that it would be easily accessible to hackers and third parties, he would have taken additional precautions to protect his PII. Plaintiff Harris received a Notice of Data Breach from Defendant dated May 28, 2021, in or about May 2021.

23. Plaintiff Brodie is a resident and citizen of Pennsylvania and was employed by Defendant in its Raleigh, North Carolina facility approximately seven years ago. Mr. Brodie, in connection with his employment, entrusted to Defendant his PII and reasonably believed Defendant would keep his PII secure. Had Defendant disclosed it would not keep his PII secure and it would be easily accessible to hackers and third parties, he would have taken additional precautions relating to his PII. He received a Notice of Data Breach from Defendant dated May 28, 2021, on or about that date.

24. Plaintiff Montelongo is a resident and citizen of the state of Illinois. Plaintiff Montelongo is a current employee of Defendant and has been employed at the Lombard, Illinois

facility since the summer of 2010. Plaintiff Montelongo, in connection with his employment, entrusted to Defendant his PII and reasonably believed Defendant would keep his PII secure. Had Defendant disclosed it would not keep his PII secure and that it would be easily accessible to hackers and third parties, he would have taken additional precautions to protect his PII. Plaintiff Montelongo received a Notice of Data Breach from Defendant dated May 28, 2021, in or around the summer of 2021.

25. Plaintiff Davis is a resident and citizen of Indiana, and was employed by Defendant at the Louisville, Kentucky location from August 2010 to December 2012. Plaintiff Davis, in connection with his employment, entrusted to Defendant his PII and reasonably believed Defendant would keep his PII secure. Had Defendant disclosed it would not keep his PII secure and that it would be easily accessible to hackers and third parties, he would have taken additional precautions to protect his PII. Plaintiff Davis received a Notice of Data Breach from Defendant dated May 28, 2021, on or about June 5, 2021.

26. Plaintiff Dudley is a resident and citizen of Texas. He was employed by Defendant in its Houston office in or about 2002 through 2006. Mr. Dudley, in connection with his employment, entrusted to Defendant his PII and reasonably believed Defendant would keep his PII secure. Had Defendant disclosed it would not keep his PII secure and it would be easily accessible to hackers and third parties, he would have taken additional precautions relating to his PII. He received a Notice of Data Breach from Defendant dated May 28, 2021, approximately one week after the letter's date.

Defendant

27. Defendant USA Waste-Management Resources, LLC is a New York limited liability company with its principal place of business in Houston, Texas. USA Waste-Management Resources, LLC is a subsidiary of, and controlled by Waste Management, Inc.

28. Waste Management describes itself as North America's leading provider of comprehensive waste management environmental services, providing services throughout the United States and Canada. Waste Management 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.

29. Waste Management'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, Waste Management is also a leading developer, operator and owner of landfill gas-to-energy facilities in the U.S.

30. Waste Management employed approximately 45,200 people in the U.S. as of December 31, 2020.[9] Waste Management owns or operates 268 landfill sites, which is the largest network of landfills in the U.S. and Canada. Waste Management manages 348 transfer stations that consolidate, compact and transport waste. Waste Management 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. Waste Management is a leading recycler in the U.S. and Canada, handling materials that include cardboard, paper, glass, plastic, and metal. Waste Management

[9] 2020 Waste Management Annual Report, pg. 8, *Available at*: http://investors.wm.com/static-files/4c8211bb-a942-4874-ac5f-a19bdd5756c9 (last visited Nov. 19, 2021).

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

31. 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.

32. This Court has personal jurisdiction over Defendant because it is a New York limited liability company, and because it conducts substantial business in this District through its offices and/or affiliates.

33. Venue is likewise proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant conduct substantial business in this District and Defendant caused harm to Class members residing in this District.

FACTUAL ALLEGATIONS

A. Defendant Collects and Stores Thousands of Current and Former Employees' (and Their Dependents') PII and Is Responsible for Its Security.

34. Defendant has locations in at least 48 states, employs approximately 45,200 people in the U.S., has tens of thousands of former employees, and is a major player in the waste management and recycling industry.[10]

35. Defendant requires its employees to provide sensitive PII as a condition of employment. Defendant's employees are also required to provide the PII of any dependents.

[10] https://careers.wm.com/internal; 2020 Waste Management Annual Report, pg. 8, Available at: http://investors.wm.com/static-files/4c8211bb-a942-4874-ac5f-a19bdd5756c9 (last visited Nov. 19, 2021).

36. At all relevant times, Defendant possessed and stored, and was legally and contractually responsible for the privacy and security, of the PII at issue in this matter.

B. Defendant's Inadequate Data Security Exposed Its Current and Former Employees' (and Their Dependents') Sensitive PII.

37. On January 21, 2021, Waste Management detected suspicious activity on its network.

38. Defendant later determined that between January 21 and 23, 2021, an unauthorized actor entered Defendant's computer network environment and accessed, viewed, and exfiltrated certain files, including past and current employee files. It was determined those files included the employees' full names, Social Security numbers (National IDs), dates of birth, and driver's license numbers. This incident is referred to herein as the "Data Breach."

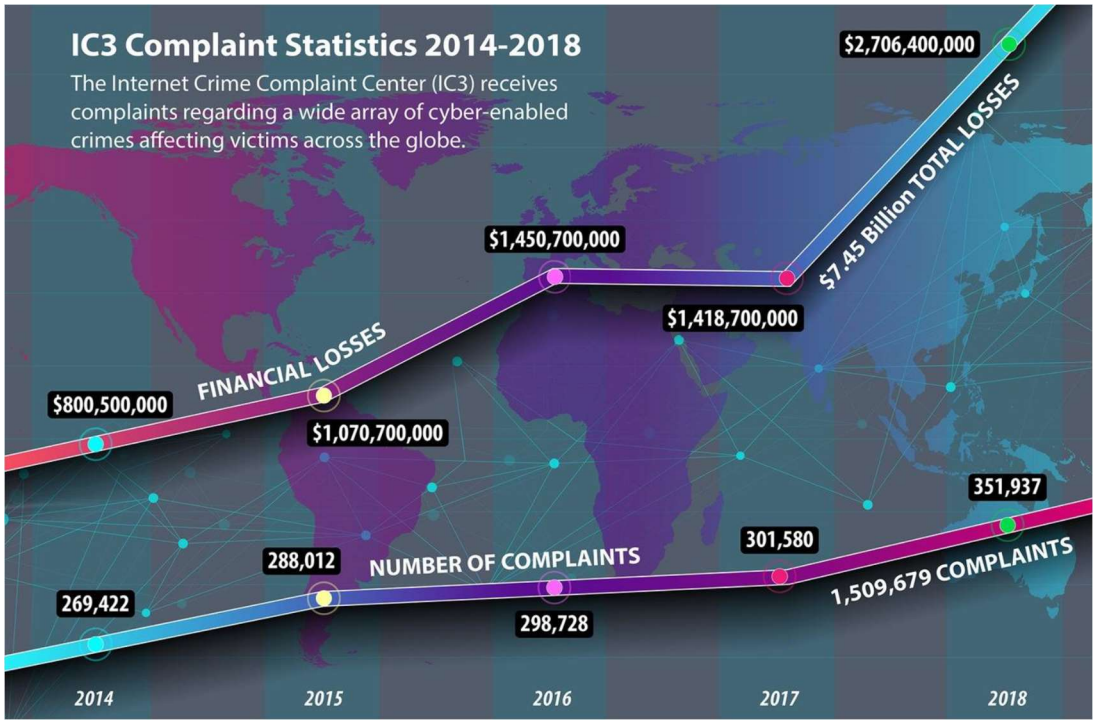
39. Despite first detecting "suspicious activity" on January 21, 2021, Defendant waited approximately *four months* to notify victims that the Data Breach had occurred. The letters Plaintiffs received providing notification of the Data Breach from Defendant were not sent until May 28, 2021.

40. After receiving the Notice Letters, it was and 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, Defendant provided "steps you may take to better protect against possible misuse of your personal information."

C. The PII Exposed by Defendant as a Result of Its Inadequate Data Security is Highly Valuable on the Black Market.

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

42. 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:



43. By 2013, it was being reported that nearly one out of four data breach notification recipients becomes a victim of identity fraud.[11]

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

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

45. 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.[12]

46. 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.[13]

47. 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.[14] Experian reports that a stolen credit or debit

[12] *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 Nov. 19, 2021).

[13] *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-dark-web/ (last visited Nov. 19, 2021).

[14] *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 Nov. 19, 2021).

card number can sell for $5 to $110 on the dark web.[15] PII has also been valued on the dark web at approximately $1 per line of information.[16] Alternatively, criminals are able to purchase access to entire company data breaches for $900 to $4,500.[17]

48. Individuals also rightfully place a high value not only on their PII, but also on the privacy of that data. Researchers have already begun to shed light on how much individuals value their data privacy—and the amount is considerable. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information between $11.33 and $16.58 per website. The study also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – $44.62."[18] This study was done in 2002, almost twenty years ago. The sea–change in how pervasive the Internet is in everyday lives since then indicates that these values—when associated with the loss of PII to bad actors—would be exponentially higher today.

49. 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

[15] *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 visited Nov. 19, 2021).

[16] https://www.pacetechnical.com/much-identity-worth-black-market/#:~:text=Personally%20identifiable%20information%20is%20sold,at%20a%20fast%20food%20joint (last visited on Nov. 19, 2021).

[17] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Nov. 19, 2021).

[18] Hann, Hui, *et al*, The Value of Online Information Privacy: Evidence from the USA and Singapore, at 17. Oct. 2002, *available at* https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited Nov. 19, 2021).

individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.

50. 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.[19]

51. The ramifications of Defendant's failure to keep Plaintiffs' and Class Members' PII secure are long lasting and severe. Because many of the data points stolen are persistent—for example, Social Security number, National ID, name, and date of birth—criminals who purchase the PII belonging to Plaintiffs and the Class Members do not need to use the information to commit fraud immediately. The PII can be used or sold for use years later, and as such Plaintiffs and Class Members will remain at risk for identity theft indefinitely.

52. What is more, it is no easy task 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.

[19] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Nov. 19, 2021).

53. 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."[20] The Social Security Administration concurs, warning:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same . . . .
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[21]

54. 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. 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

[20] 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 Nov. 19, 2021).

[21] SSA, Identity Theft and Your Social Security Number, SSA Publication No. 05-10064 (Dec. 2013), *available at*: http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Nov. 19, 2021).

credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[22]

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

56. 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."[23]

57. 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.

58. 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.

59. 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,

---

[22] 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 Nov. 19, 2021).

[23] 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 Nov. 19, 2021).

receive government benefits, and make purchases and secure credit in a victim's name.[24] 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 and inconveniences repairing damage to their credit records . . . [and their] good name."[25]

D. Data Breaches Have Become More Prevalent.

60. The frequency of cyberattacks has increased significantly in recent years.[26] In fact, "Cyberattacks rank as the fastest growing crime in the US, causing catastrophic business disruption. Globally, cybercrime damages are expected to reach US $6 trillion by 2021."[27]

61. Cybersecurity Ventures, a leading researcher on cybersecurity issues,

> expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined.[28]

[24] *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 Nov. 19, 2021).

[25] *Id*.

[26] *See* https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50 (last visited Nov. 19, 2021).

[27] https://www.isaca.org/resources/news-and-trends/industry-news/2020/top-cyberattacks-of-2020-and-how-to-build-cyberresiliency (last visited Nov. 19, 2021) (citing Cybersecurity Ventures, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016).

[28] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016 (last visited Nov. 19, 2021).

62. As noted in recent reports by Deloitte and Interpol, cyberattacks have greatly increased in the wake of the COVID-19 pandemic.[29]

E. Defendant Failed to Comply with Federal Trade Commission Requirements.

63. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[30] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[31]

64. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, applying and opening credit card accounts, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

65. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial

[29] https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html (last visited Nov. 19, 2021); https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats (last visited Nov. 19, 2021).

[30] See *Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2012), http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited Nov. 19, 2021).

[31] https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Nov. 19, 2021). The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. 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." *Id*.

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.[32]

66. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, establishing guidelines for fundamental data security principles and practices for business.[33] 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.[34]

67. 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; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[35]

---

[32] *See* Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Nov. 19, 2021).

[33] *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 Nov. 19, 2021).

[34] *Id*.

[35] Federal Trade Commission, *Start With Security*, *supra*, footnote 31.

68. 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.[36]

69. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the GAO Report:

> [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.[37]

70. Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it, and the foreseeable consequences if its data security systems were breached. However, Defendant failed to take adequate cyber security measures to prevent the Data Breach from occurring.

71. By being negligent in securing Plaintiffs' and Class members' PII and allowing an unauthorized actor to access its computer network environment, Defendant failed to employ

[36] 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 Nov. 19, 2021).

[37] *See* https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07-737/html/GAOREPORTS-GAO-07-737.htm (last visited Nov. 19, 2021).

reasonable and appropriate measures to protect against unauthorized access to confidential employee data. Defendant's data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

F. Plaintiffs' Experiences.

Plaintiff Marcaurel

72. Plaintiff Marcaurel was employed by Defendant 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.

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

74. 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.

75. Plaintiff Marcaurel has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, including 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.

76. Plaintiff Marcaurel is very careful about sharing her PII. She 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.

77. Plaintiff Marcaurel stores documents containing her PII in a safe and secure location.

78. 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 Defendant 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.

79. 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.

80. 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.

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

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

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

Plaintiff Fierro

84. Plaintiff Fierro is a current employee of Defendant at its facility located in Chino, California, and has worked for Defendant since August 2019, as a residential truck driver.

85. In or about June 2021, Plaintiff Fierro received the Notice Letter from Defendant informing him of the Data Breach.

86. After receiving notification of the Data Breach, Plaintiff Fierro noticed an uptick in the amount and frequency of spam calls he was receiving. Plaintiff Fierro also spent time researching the Data Breach, and reviewing and monitoring his credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. This is valuable time that Plaintiff Fierro otherwise would have spent on other activities.

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

88. Plaintiff Fierro is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. He deletes any and all electronic documents containing his PII and destroys any documents that may contain any of his PII, or that may contain any information that could otherwise be used to compromise his PII.

89. Plaintiff Fierro stores documents containing his PII in a safe and secure location.

90. Plaintiff Fierro has suffered actual injury in the form of damages to, and diminution in, the value of his PII—a form of intangible property that Plaintiff Fierro entrusted to Defendant for the purpose of his employment well over two years ago. This PII was compromised in, and has been diminished as a result of, the Data Breach.

91. Plaintiff Fierro 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 his privacy and the substantial risk of fraud and identity theft which he now faces.

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

93. Knowing thieves stole his PII, including his Social Security number, driver's license number and other PII he was required to provide to Defendant, and knowing that his PII will likely be sold on the dark web, has caused Plaintiff Fierro great anxiety.

94. Plaintiff Fierro has a continuing interest in ensuring his PII which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

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

Plaintiff Ingram

96. Plaintiff Ingram was employed by Defendant at its Phoenix Call Center located in Phoenix, Arizona from on about June 29, 2005 through January 19, 2020 handling collections in the billing department.

97. On or about June 8, 2021, Plaintiff Ingram was informed by a friend about the Data Breach. Plaintiff Ingram contracted Defendant's Human Resources on or about June 9, 2021, to determine whether she was involved in the data breach. Defendant informed her that she should have already received a Notice of Data Breach. Plaintiff Ingram had not received the notice and had to request Defendant retransmit the June 4, 2021 Notice of Data Breach to her twice before she eventually received it via mail.

98. After the Data Breach, Plaintiff Ingram noticed an uptick in the amount and frequency of phishing telephone calls and emails she was receiving, including all manner of other phishing, scam, and spam communications. Plaintiff Ingram has also experienced several forms of identity theft she believes are due to the Data Breach. An unauthorized third party used her PII to claim pandemic assistance unemployment benefits in Ohio, a state which she has never lived in or visited. Also, in or around July 2021, Plaintiff Ingram had an account opened with Cox Communications in her name by unknown person. This fraudulent account resulted in claims of unpaid bills by Cox Cable on her Credit Reports. Then, beginning on or about September 1, 2021, an unauthorized third party signed into Plaintiff Ingram's Netflix account, changed the password and language, changed the location to Huila, Colombia, and charged the new subscription to her payment card, including an additional "international charge." These charges equal $10.85 plus an additional $1.00 "international charge" for the international usage of her payment card. Plaintiff

Ingram had to place a freeze on her credit because of the identity theft she experienced as a result the Data Breach.

99. Plaintiff Ingram has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, including spending time on the telephone and sorting through her unsolicited emails, addressing her inaccurate credit reports due to the Cox Communication account, communicating with the State of Ohio to report the fraudulent pandemic unemployment insurance benefit claims, contacting Netflix to recover her account from the unknown person in Colombia who stole it, contacting her bank in order to report the charges due to the theft of her Netflix account as fraudulent, researching the Data Breach, contacting the credit bureaus to freeze her credit, contacting Defendant in order to have it send her Notice of Data Breach letter, 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.

100. Plaintiff Ingram is very careful about sharing her PII. She 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.

101. Plaintiff Ingram stores documents containing her PII in a safe and secure location.

102. 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 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.

103. 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.

104. Plaintiff Ingram has suffered present, 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 is now in the hands of cyber criminals and other unauthorized third parties.

105. Plaintiff Ingram has already suffered injury in the form of fraud, identity theft, and misuse of her PII resulting from the compromise of her PII, including fraudulent claims for unemployment insurance in a state she never resided in, a fraudulent account with Cox Communications resulting in the impairment of her credit, and fraudulent usage and charges to her Netflix account and credit card.

106. Knowing thieves stole her PII, including her Social Security number, driver's license number, and other PII she was required to provide to Defendant, and knowing that her PII has likely already been sold on the dark web, has caused Plaintiff Ingram great anxiety.

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

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

Plaintiff Krenzer

109. Plaintiff Krenzer was employed by Defendant at the corporate headquarters in Houston, Texas in or about 2008 through 2104, as a Senior Financial Analyst.

110. Shortly after June 4, 2021, Plaintiff Krenzer received the Notice Letter from Defendant informing him of the Data Breach.

111. After receiving notification of the Data Breach, Plaintiff Krenzer began receiving telephone calls from people claiming to be debt collectors from Amazon.com, who were attempting to collect a debt owed to Amazon.com by Mr. Krenzer. Plaintiff Krenzer, however, confirmed that he did not have a debt outstanding with Amazon.com. Plaintiff Krenzer also began receiving telephone calls from people claiming to be debt collectors from the U.S. Internal Revenue Service ("IRS"), who were attempting to collect a debt owed to the IRS by Plaintiff Krenzer. Again, Plaintiff Krenzer confirmed that he did not have an outstanding debt with the IRS. Plaintiff Krenzer also began receiving telephone calls from Spanish speakers. He does not speak Spanish. Plaintiff Krenzer also noticed an increase in the frequency of phishing emails he was receiving.

112. Plaintiff Krenzer has been forced to spend at least 15 hours—and counting—dealing with and responding to the direct consequences of the Data Breach, including spending time on the telephone with unsolicited telephone debt collection calls, researching phony debt collection allegations, and sorting through unsolicited phone messages and emails, researching the Data Breach, exploring credit monitoring and identity theft insurance options, signing up for credit monitoring and identify theft insurance, and signing up for an annual subscription for a spam telephone call blocker service for which he is paying $19.99 per month, and self–monitoring his bank and credit card accounts. This is time that has been lost forever and cannot be recaptured.

113. Plaintiff Krenzer is very careful about sharing his PII. He does not knowingly transmit unencrypted PII over the internet or any other unsecured source. He deletes electronic documents containing his PII and destroys any documents that may contain any of his PII, or that may contain any information that could otherwise be used to compromise his PII.

114. Plaintiff Krenzer stores documents containing his PII in a safe and secure location.

115. Plaintiff Krenzer has suffered actual injury in the form of damages to, and diminution in, the value of his PII—a form of intangible property Plaintiff Krenzer entrusted to Defendant for the purpose of his employment which began approximately 13 years ago. This PII was compromised in, and has been diminished as a result of, the Data Breach.

116. Plaintiff Krenzer has also suffered actual injury in the forms of out-of-pocket damages for the purchase of a telephone spam call blocker (at $19.99 per month), 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 his privacy and the substantial risk of fraud and identity theft which he now faces.

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

118. Knowing thieves stole his PII, including his Social Security number, driver's license number, and other PII he was required to provide to Defendant, and knowing that his PII will likely be sold on the dark web, has caused Plaintiff Krenzer great anxiety.

119. Plaintiff Krenzer has a continuing interest in ensuring his PII which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

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

Plaintiff Fusilier

121. Plaintiff Fusilier was employed by Defendant in the sustainability division in Houston, Texas.

122. In June 2021, Plaintiff Fusilier received the Notice Letter dated June 4, 2021, from Defendant informing her of the Data Breach.

123. After receiving notification of the Data Breach, Plaintiff Fusilier noticed an uptick in the amount and frequency of phishing emails she was receiving, including a suspicious and unsolicited email from the Texas unemployment office. Furthermore, since the Data Breach, Plaintiff Fusilier has experienced suspicious and increased targeting through autodialed phone calls—including voice recordings purportedly from the Internal Revenue Service and Social Security Administration. Additionally, in November 2021, she received an email from Chase, with whom she has a credit card account, notifying her of a transaction on Walmart.com charged to her Chase credit card, and asking Plaintiff Fusilier to confirm whether she recognized the charge. Plaintiff Fusilier did not recognize the charge and contacted Chase to inform it she did not make and/or authorize any purchase from Walmart.com. Due to the fraudulent charge to her credit card, Plaintiff Fusilier's credit card was cancelled and she was issued a new card.

124. Plaintiff Fusilier has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, including spending time on the telephone and sorting through her unsolicited emails and phone calls, resolving fraudulent charges on her credit card, 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.

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

126. Plaintiff Fusilier stores documents containing her PII in a safe and secure location.

127. Plaintiff Fusilier has suffered actual injury in the form of damages to, and diminution in, the value of her PII—a form of intangible property Plaintiff Fusilier entrusted to Defendant for the purpose of her employment over five years ago. This PII was compromised in, and has been diminished as a result of, the Data Breach.

128. Plaintiff Fusilier 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.

129. Plaintiff Fusilier 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 is now in the hands of cyber criminals and other unauthorized third parties.

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

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

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

Plaintiff Harris

133. Plaintiff Harris was employed by Defendant as a National Account Executive traveling throughout the United States, Canada, and Mexico, from 1998 through 2005.

134. In May 2021, Plaintiff Harris learned of the Data Breach while reading online news.

135. After learning about the Data Breach online, Plaintiff Harris checked his NortonLifeLock service. Plaintiff Harris learned that NortonLifeLock received hits on February 19, 20, and 21, 2021 indicating his personal information had been sold amongst dark web information groups. Between February 2021 and July 2021, three (3) attempts were made to file for Illinois unemployment benefits in Plaintiff Harris' name. These criminal attempts required Plaintiff Harris to spend time dealing with and responding to the fraudulent benefit claims.

136. Approximately two days after reading the online news about the Data Breach, Plaintiff Harris received the Notice Letter dated May 28, 2021, from Defendant informing him of the Data Breach.

137. After receiving notification of the Data Breach, Plaintiff Harris noticed an uptick in the amount and frequency of phishing emails and text messages he was receiving, and he has experienced suspicious and increased targeting through autodialed phone calls.

138. Plaintiff Harris has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, including spending time on the telephone and sorting through his unsolicited emails, text messages, and phone calls, researching the Data Breach, monitoring his NortonLifeLock service and exploring identity theft insurance options, and self-monitoring his accounts. This is time that has been lost forever and cannot be recaptured.

139. Plaintiff Harris is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

140. Plaintiff Harris stores documents containing his PII in a safe and secure location.

141. Plaintiff Harris has suffered actual injury in the form of damages to, and diminution in, the value of his PII—a form of intangible property Plaintiff Harris entrusted to Defendant for the purpose of his employment over five years ago. This PII was compromised in, and has been diminished as a result of, the Data Breach.

142. Plaintiff Harris 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 his privacy and the substantial risk of fraud and identity theft which he now faces.

143. Plaintiff Harris has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII resulting from the compromise of his PII, especially his Social Security number, in combination with his full name

and driver's license number, which is now in the hands of cyber criminals and other unauthorized third parties.

144. Knowing thieves stole his PII, including his Social Security number, driver's license number, and other PII he was required to provide to Defendant, and knowing that his PII will likely be sold on the dark web, has caused Plaintiff Harris great anxiety.

145. Plaintiff Harris has a continuing interest in ensuring his PII which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

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

Plaintiff Brodie

147. Plaintiff Brodie was employed by Defendant in its Raleigh, North Carolina facility approximately 7 years ago.

148. A few days after May 28, 2021, Plaintiff Brodie received the Notice Letter from Defendant informing him of the Data Breach.

149. In approximately February 2021, an unknown third party made a series of unauthorized purchases with his Amazon account, which resulted in fraudulent charges totaling over $4,000 to his debit card. These fraudulent transactions resulted in losses from Plaintiff Brodie's checking account that have not been reimbursed by his bank or by Amazon. Plaintiff Brodie believes these fraudulent charges are a direct result of the Data Breach.

150. Furthermore, since approximately April or May 2021, the number of suspicious phone calls and emails Plaintiff Brodie receives has dramatically increased. Plaintiff Brodie also

recently received numerous notifications from ID.me that someone has been attempting to make fraudulent purchases using his identity with his debit card. For example, he was recently notified by ID.me that someone attempted to purchase a timeshare using his identity.

151. As a result of the Data Breach, Plaintiff Brodie has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, including spending time on the telephone with his bank and with Amazon, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self–monitoring his accounts. This is time that has been lost forever and cannot be recaptured.

152. Plaintiff Brodie is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. He deletes any and all electronic documents containing his PII and destroys any documents that may contain any of his PII or that may contain any information that could otherwise be used to compromise his PII.

153. Plaintiff Brodie stores documents containing his PII in a safe and secure location.

154. Plaintiff Brodie has suffered actual injury in the form of out-of-pocket losses totaling over $4,000, and damages to, and diminution in, the value of his PII—a form of intangible property that Plaintiff Brodie entrusted to Defendant for the purpose of his employment. This PII was compromised in, and has been diminished as a result of, the Data Breach.

155. Plaintiff Brodie 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 his privacy and the substantial risk of fraud and identity theft that he now faces.

156. Plaintiff Brodie has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII resulting from the

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

157. Knowing that thieves stole his PII, including his Social Security Number, driver's license number and other PII that he was required to provide to Defendant, and knowing that his PII will likely be sold on the dark web, has caused Plaintiff Brodie great anxiety.

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

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

Plaintiff Montelongo

160. Plaintiff Montelongo is currently employed by Defendant at its Lombard, Illinois facility, where he has worked since the summer of 2010. Plaintiff Montelongo works as a Router/Dispatcher.

161. A few days after May 28, 2021, Plaintiff Montelongo received the Notice Letter information him of the Data Breach.

162. Shortly before receiving the Notice Letter, Plaintiff Montelongo noticed an increase in suspicious emails and "robo" calls targeting him in apparent phishing scams.

163. Furthermore, following the notification of the Date Breach, Plaintiff Montelongo experienced actual identity fraud. Specifically, in September, 2021, he noticed two false charges on his credit card. Plaintiff Montelongo had to cancel this card after each false charge.

164. Plaintiff Montelongo has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, including spending time on unsolicited telephone calls and sorting through his unsolicited emails, researching the Data Breach, exploring additional credit monitoring and identity theft insurance options, cancelling credit cards, working with his bank to resolve unauthorized transaction, and self–monitoring his accounts. This is time that has been lost forever and cannot be recaptured.

165. Plaintiff Montelongo is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. He deletes any and all electronic documents containing his PII and destroys any documents that may contain any of his PII, or that may contain any information that could otherwise be used to compromise his PII.

166. Plaintiff Montelongo stores documents containing his PII in a safe and secure location.

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

168. Plaintiff Montelongo 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 his privacy and the substantial risk of fraud and identity theft which he now faces.

169. Plaintiff Montelongo has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII resulting from the compromise of his PII, especially his Social Security number, in combination with his full name

and driver's license number, which is now in the hands of cyber criminals and other unauthorized third parties.

170. Knowing thieves stole his PII, including his Social Security number, driver's license number, and other PII he was required to provide to Defendant, and knowing that his PII will likely be sold on the dark web for use in future crimes to target his identity, has caused Plaintiff Montelongo great anxiety.

171. Plaintiff Montelongo has a continuing interest in ensuring his PII which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

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

Plaintiff Davis

173. Plaintiff Davis was previously employed by Defendant at its Louisville, KY facility, where he worked from August 2010 to January 2013, as an Account Manager for the Sales Department

174. A few days after May 28, 2021, Plaintiff Davis received the Notice Letter information him of the Data Breach.

175. Shortly before receiving the Notice Letter, Plaintiff Davis noticed an increase in suspicious emails and texts targeting him in apparent phishing scams around the beginning of the year.

176. Plaintiff Davis has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, including spending time on unsolicited telephone calls

and texts, and sorting through his unsolicited emails, researching the Data Breach, and self-monitoring his accounts. This is time that has been lost forever and cannot be recaptured.

177. Plaintiff Davis is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. He deletes any and all electronic documents containing his PII and destroys any documents that may contain any of his PII, or that may contain any information that could otherwise be used to compromise his PII.

178. Plaintiff Davis stores documents containing his PII in a safe and secure location.

179. Plaintiff Davis has suffered actual injury in the form of damages to, and diminution in, the value of his PII—a form of intangible property Plaintiff Davis entrusted to Defendant for the purpose of his employment. This PII was compromised in, and has been diminished as a result of, the Data Breach.

180. Plaintiff Davis 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 his privacy and the substantial risk of fraud and identity theft which he now faces.

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

182. Knowing thieves stole his PII, including his Social Security number, driver's license number, and other PII he was required to provide to Defendant, and knowing that his PII

will likely be sold on the dark web for use in future crimes to target his identity, has caused Plaintiff Davis great anxiety.

183. Plaintiff Davis has a continuing interest in ensuring his PII which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

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

Plaintiff Dudley

185. Plaintiff Dudley was employed by Defendant at its Houston office in or about 2002 through 2006 as an LMS Database Administrator and Web-Based Training Developer.

186. Approximately one week after May 28, 2021, Plaintiff Dudley received the Notice Letter from Defendant informing him of the Data Breach.

187. After receiving notification of the Data Breach, Plaintiff Dudley noticed increased targeting through autodialed phone calls. Incoming phone calls are often labelled "Spam Risk."

188. Plaintiff Dudley has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, including spending time on the telephone, researching the Data Breach, exploring credit monitoring and identity theft monitoring options, and self-monitoring his accounts. This is time that has been lost forever and cannot be recaptured.

189. Plaintiff Dudley is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

190. Plaintiff Dudley stores documents containing his PII in a safe and secure location.

191. Plaintiff Dudley has suffered actual injury in the form of damages to, and diminution in, the value of his PII—a form of intangible property Plaintiff Dudley entrusted to Defendant for the purpose of his employment over 15 years ago. This PII was compromised in, and has been diminished permanently as a result of, the Data Breach.

192. Plaintiff Dudley 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 his privacy and the substantial risk of fraud and identity theft which he now faces.

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

194. Knowing thieves stole his PII, including his Social Security number, driver's license number, and other PII he was required to provide to Defendant, and knowing that his PII will likely be sold on the dark web, has caused Plaintiff Dudley great anxiety.

195. Plaintiff Dudley has a continuing interest in ensuring his PII which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

196. As a result of the Data Breach, Plaintiff Dudley is presently and 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 Class Members Suffered Damages.

197. The ramifications of Defendant's 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.[38]

198. The PII belonging to Plaintiffs and Class members is private, sensitive in nature, and was left inadequately protected by Defendant 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.

199. As a requisite of obtaining employment, Defendant 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 Defendant to ensure that the PII of Plaintiffs and Class members in its possession was only used to provide the agreed–upon compensation and other employment benefits from Defendant.

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

201. The Data Breach was a direct and proximate result of Defendant'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

[38] *2014 LexisNexis True Cost of Fraud Study, available at:* https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last visited Nov. 19, 2021).

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.

202. Defendant had the resources necessary to prevent the Data Breach, but neglected to implement adequate data security measures, despite its obligations to protect current and former employees' (and their dependents') PII, and despite its public statements that it is "dedicate[ed] to safety" and one of the "world's most ethical companies" for the twelfth year in a row.[39]

203. Had Defendant remedied the deficiencies in its data security training and protocols, and adopted security measures recommended by experts in the field, it would have prevented the intrusion leading to the theft of PII.

204. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class members have been placed at a current, and 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.

205. 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

[39] http://investors.wm.com/news-releases/news-release-details/ethisphere-announces-waste-management-one-2021-worlds-most (last visited Nov. 17, 2021).

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;

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

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

206. 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.

207. To date, other than providing a woefully inadequate twelve (12) months of credit monitoring and identity protection services, Defendant does 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.

208. Defendant's 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. Defendant's Notice Letter indicates it is putting the burden on Plaintiffs and Class members to discover possible fraudulent activity and identity theft.

209. Defendant's 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.[40] 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 Defendant'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

210. Plaintiffs bring all claims as Class claims under Federal Rule of Civil Procedure 23. The requirements of Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3) are met with respect to the classes defined below.

211. 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, or any of its affiliates, and had their PII compromised as a result of the Data Breach that occurred between January 21 and 23, 2021 (the "Nationwide Class").

[40] *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 Nov. 19, 2021).

212. Pursuant to Rule 23, Plaintiffs Marcaurel and Fierro also assert claims on behalf of a separate statewide California subclass, defined as follows:

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

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

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

215. Plaintiffs reserve the right to modify and/or amend the Class or Subclass definitions, including but not limited to adding additional subclasses, as necessary.

216. **Numerosity.** Members of the proposed Class likely number in the hundreds of thousands and are thus too numerous to practically join in a single action. Defendant reported that 268,510 persons have been affected by the Data Breach.[41]

217. Upon information and belief, the California Class includes at least hundreds of individuals whose personal data was entrusted to Defendant and compromised in the Data Breach.

218. Membership in the Class is readily ascertainable from Defendant's own records, including addresses and other contact information which can be used to provide notice to the Class.

219. **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:

[41] *See* **Exhibit A,** Office of the Maine Attorney General, *Data Breach Notifications*.

a. whether Defendant engaged in the wrongful conduct alleged herein;

b. whether Defendant's inadequate data security measures were a cause of the Data Breach;

c. whether Defendant's conduct was negligent;

d. whether Defendant's conduct was unlawful;

e. whether Defendant owed a legal duty to Plaintiffs and the other Class members to exercise due care in collecting, storing, and safeguarding their PII;

f. whether Defendant owed a contractual duty to Plaintiffs and the other Class members to protect their PII;

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

h. whether Defendant breached contractual duties owed to Plaintiffs and the Class members to protect their PII;

i. whether Defendant had a duty to provide prompt and accurate notice of the Data Breach to Plaintiffs and the Class;

j. whether Defendant breached its duty to provide prompt and accurate notice of the Data Breach to Plaintiffs and the Class;

k. whether Plaintiffs and the Class are at a present and/or future increased risk for identity theft because of the Data Breach;

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

m. whether Plaintiffs and Class Members suffered injury, including ascertainable losses, as a result of Defendant's conduct (or failure to act);

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

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

220. Defendant 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 common questions in this action.

221. The 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. Defendant's misconduct impacted all Class members in the same manner.

222. **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.

223. **Predominance.** The questions of law and fact common to Class Members predominate over any questions which may affect only individual members.

224. **Injunctive Relief.** Defendant acted and/or refused to act on grounds generally applicable to the Class, making Class–wide injunctive and/or declaratory relief appropriate under Fed. Civ. P. 23(b)(2).

225. **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 foreseen in managing 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 Defendant, making it impracticable for Class members to individually seek redress for Defendant's 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.

226. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual members of the Class, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

227. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A) because the prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a Class action conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

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

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

229. Defendant 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 their data security systems to ensure that Plaintiffs' and Class members' PII in Defendant's possession was adequately secured and protected.

230. Defendant owed a duty of care to Plaintiffs and members of the Class to provide security, consistent with industry standards, to ensure their protocols, systems, and networks adequately protected the PII of its current and former employees.

231. Defendant owed a duty of care to Plaintiffs and Class members because they were foreseeable and probable victims of any inadequate data security practices. Defendant 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.

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

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

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

235. Defendant breached its 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.

236. Plaintiffs' injuries and damages, as described below, are a reasonably certain consequence of Defendant's breach of its duties.

237. Because Defendant knew that a breach of its systems would damage thousands of its current and former employees, Defendant had a duty to adequately protect its data systems and the PII contained therein.

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

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

240. In engaging in the negligent acts and omissions as alleged herein, which permitted an "unauthorized actor" to access Defendant's network environment, Defendant 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 Defendant failed to do as discussed herein.

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

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

243. As a direct and proximate cause of Defendant's actions and inactions, including but not limited to its failure to properly encrypt its 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:

a. actual identity theft;

b. the loss of the opportunity to determine for themselves how their PII is used;

c. the compromise, publication, and/or theft of their PII;

d. 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;

e. 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;

f. costs associated with placing freezes on credit reports and password protection;

g. anxiety, emotional distress, loss of privacy, and other economic and non-economic losses;

h. the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of employees and former employees in its continued possession; and

i. 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 Contract
(On behalf of Plaintiffs and the Nationwide Class)

244. Plaintiffs incorporate paragraphs 1 through 227 as though fully set forth herein.

245. Defendant knew or should have known the PII Plaintiffs and Class members provided to Defendant was highly confidential and sensitive and that Defendant had a contractual duty to protect the PII.

246. As a condition of employment, Plaintiffs and Class members were required to provide their PII to Defendant and sign a written contractual agreement, referred to as the Employee Handbook, which includes the terms and conditions of employment.

247. Defendant's current and former employees, including Plaintiffs and Class members, worked for and gave their PII to Defendant as a condition of employment. Plaintiffs and Class members therefore demonstrated their willingness and intent to enter into a bargain with Defendant, and assent to the terms of the agreement encompassing Defendant's policies and

procedures, by working for Defendant and giving their PII to Defendant in exchange for wages and benefits. Plaintiffs and Class members therefore entered into a contractual agreement with Defendant.

248. The agreement between Waste Management, on one hand, and Plaintiffs and Class members on the other, includes specific language regarding employee privacy and the confidentiality of the company's affairs, which includes the handling and protection of Plaintiffs' and Class members' PII.[42] The agreement states: employee PII is treated as "confidential" information; individuals with access to confidential information must protect it from disclosure; confidential information should only be stored in access–restricted and protected areas; it is only to be shared with authorized people; and unauthorized disclosure is a violation of company policy and may result in legal action against Defendant and/or individuals involved. The Handbook further addresses employee privacy, stating employee information, including information about their employment, is considered private and is only to be used for valid business purposes. The agreement further states Defendant knew that allowing outside computer connections to its computer network—which it did—created the additional risk of unauthorized access.

249. Plaintiffs and Class members have upheld their obligations under the agreement. Waste Management, on the other hand, breached its obligations by failing to implement reasonable security measures, which led to unauthorized disclosure of Plaintiffs' and Class members' PII to third parties. Defendant further breached the agreement by failing to treat PII as "confidential," failing to protect that information from disclosure to unauthorized parties, failing to restrict access to the PII, and allowing the PII in its possession to be used for non–business purposes. By the

[42] The agreement also states it is not to be reproduced or distributed outside of Waste Management without the company's approval.

terms of the agreement, Waste Management allowing the unauthorized disclosure is a violation of the company policy and a breach of the agreement.

250. As a direct and proximate result of Defendant's breach of the agreement, Plaintiffs and Class members did not receive the benefit of their bargain with Defendant, and were injured as described in detail herein.

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

251. Plaintiffs incorporate paragraphs 1 through 227 as though fully set forth herein.

252. Defendant 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.

253. Defendant 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 Defendant to ensure that the PII of Plaintiffs and Class members in its possession was only used to provide the agreed–upon compensation and other employment benefits.

254. 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 Defendant.

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

256. 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 Defendant but for the prospect of Defendant's promise of compensation and other employment benefits. Conversely, Defendant presumably would not have taken Plaintiffs' and Class members' PII if it did not intend to provide Plaintiffs and Class members compensation and other employment benefits, or, in the case of applicants, consider hiring them.

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

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

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

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

261. Defendant's 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.

262. Defendant was on notice that its systems and data security protocols could be inadequate, yet failed to invest in the proper safeguarding of Plaintiffs' and Class members' PII.

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

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

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

265. Plaintiffs incorporate paragraphs 1 through 227 as though fully set forth herein.

266. At all times during Plaintiffs' and Class members' interactions with Defendant as its employees, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and Class members' PII that Plaintiffs and Class members provided to Defendant.

267. 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.

268. As alleged herein and above, Defendant's 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.

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

270. Defendant requested and 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.

271. Due to Defendant's 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.

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

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

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

275. The injury and harm Plaintiffs and Class members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class members' PII. Defendant knew its 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 at risk.

276. As a direct and proximate result of Defendant's 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 loss of the opportunity to determine for themselves how their PII is used;

c. the compromise, publication, and/or theft of their PII;

d. 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;

e. 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;

f. costs associated with placing freezes on credit reports and password protection;

g. anxiety, emotional distress, loss of privacy, and other economic and non-economic losses;

h. the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of employees and former employees in its continued possession; and

i. 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.

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

277. Plaintiffs incorporate paragraphs 1 through 227 as though fully set forth herein.

278. In light of their special relationship, Defendant became the guardian of Plaintiffs' and Class members' PII. Defendant became a fiduciary, created by its undertaking and guardianship of its 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.

279. In order to provide Plaintiffs and Class members compensation and employment benefits, or to consider Plaintiffs and Class members for employment, Defendant required Plaintiffs and Class members to provide their PII to Defendant.

280. Defendant 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.

281. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of their relationship with them. Defendant breached its fiduciary

duties owed to Plaintiffs and Class members by failing to properly encrypt and otherwise protect Plaintiffs' and Class members' PII. Defendant further breached its 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.

282. As a direct and proximate result of Defendant's breaches of its 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 to determine for themselves how their PII is used;

c. the compromise, publication, and/or theft of their PII;

d. 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;

e. 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;

f. costs associated with placing freezes on credit reports and password protection;

g. anxiety, emotional distress, loss of privacy, and other economic and non-economic losses;

h. the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to

undertake appropriate and adequate measures to protect the PII of employees and former employees in its continued possession; and

i. 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.

283. As a direct and proximate result of Defendant's breach of its 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
Unjust Enrichment
(On behalf of Plaintiffs and Nationwide Class)

284. Plaintiffs incorporate paragraphs 1 through 227 as though fully set forth herein.

285. By engaging in the conduct described herein, Defendant knowingly obtained benefits from Plaintiffs and Class members, namely their labor and the profits therefrom, and actual monies and other benefits under circumstances such that it would be inequitable and unjust for Defendant to retain the benefits.

286. By engaging in the acts and omissions described herein, Defendant was knowingly enriched by the costs savings resulting from failing to reasonably expended monies to protect Plaintiffs' and Class members' PII. Defendant knew or should have known that theft of employee PII could happen, yet Defendant failed to take reasonable steps to pay for the level of security required and/or industry standard security to prevent the Data Breach.

287. By engaging in the conduct described herein, Defendant knowingly obtained benefits from Plaintiffs and Class members under circumstances such that it would be inequitable and unjust for Defendant to retain the benefits.

288. Defendant will be unjustly enriched if it is permitted to retain the benefits derived from the theft of Plaintiffs' and Class members' PII.

289. Plaintiffs and each Class member are therefore entitled to an award of compensatory damages in an amount to be determined at trial, or the imposition of a constructive trust upon the monies derived by Defendant by means of the above–described actions.

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

290. Plaintiffs incorporate paragraphs 1 through 227 as though fully set forth herein.

291. Plaintiffs bring this cause of action under the federal Declaratory Judgment Act, 28 U.S.C. § 2201.

292. As previously alleged, Plaintiffs and Class members entered into an implied contract requiring Defendant to provide adequate security for the PII it collected from Plaintiffs and Class members.

293. Defendant owes a duty of care to Plaintiffs and Class members, requiring Defendant to adequately secure Plaintiffs' and Class members' PII.

294. Defendant still possess Plaintiffs' and Class members' PII.

295. Since the Data Breach, Defendant has announced few if any changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices that permitted the Data Breach to occur and, thereby, prevent future data breaches.

296. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and Class members. In fact, now that Defendant's insufficient data security is known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack.

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

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

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

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

b. engage third–party security auditors and internal personnel to run automated security monitoring;

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

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

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

f. conduct regular computer system scanning and security checks;

g. 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. to meaningfully educate its 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.

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

300. Plaintiffs Marcaurel and Fierro ("California Plaintiffs") incorporate paragraphs 1 through 227 as though fully set forth herein..

301. Defendant violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent the unauthorized access, exfiltration, theft, and/or disclosure of California Plaintiffs' and California Class members' PII as a result of Defendant's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect California Plaintiffs' and California Class members' PII.

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

303. As a direct and proximate result of Defendant's acts and/or failures to act, California Plaintiffs and California Class members were injured and lost money or property, including but not limited to the loss of California Plaintiffs' and California Class members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

304. Defendant knew or should have known that its network computer systems and data security practices were inadequate to safeguard California Plaintiffs' and California Class members' PII, and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect California Plaintiffs' and California Class members' PII.

305. Defendant is organized for the profit or financial benefit of its owners and collects PII as defined in Cal. Civ. Code § 1798.140.

306. California Plaintiffs and California Class members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards California Plaintiffs' and California Class members' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold California Plaintiffs' and California Class members' PII. California Plaintiffs and California Class members have an interest in ensuring their PII is reasonably protected.

307. On June 21, 2021, and July 19, 2021, Plaintiff Marcaurel's counsel and Plaintiff Fierro's counsel, respectively, each sent a notice letter to Defendant's registered service agent via

certified mail. On information and belief Defendant did not cure the Data Breach within 30 days, and California Plaintiffs believe any such cure was not possible under these facts and circumstances. California Plaintiffs 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.

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

308. California Plaintiffs incorporate paragraphs 1 through 227 as though fully set forth herein.

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

310. Defendant stored California Plaintiffs' and California Class members' PII in its network environment. Defendant falsely represented to California Plaintiffs and California Class members that their PII was secure and would remain private or, alternatively, failed to disclose to California Plaintiffs and California Class members that their PII was not secure.

311. Defendant knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations and that would have kept California Plaintiffs' and California Class members' PII secure and prevented the loss or misuse of that PII.

312. Even without these misrepresentations and omissions, California Plaintiffs and California Class members were entitled to assume, and did assume, Defendant would take appropriate measures to keep their PII safe. Defendant did not disclose at any time that California

Plaintiffs' and California Class members' PII was vulnerable to hackers because Defendant's data security measures were inadequate and most likely outdated, and Defendant was the only one in possession of that material information, which it had a duty to disclose.

Unlawful Business Practices

313. Defendant 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 its network environment, specifically the security thereof, and its ability to safely store California Plaintiffs' and California Class members' PII.

314. Defendant 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 California Plaintiffs and California Class members of the Data Breach.

315. Defendant also violated California Civil Code § 1798.81.5(b) in that it failed to maintain reasonable security procedures and practices.

316. If Defendant had complied with these legal requirements, California Plaintiffs and California Class members would not have suffered the damages related to the Data Breach, and from Defendant's failure to timely notify California Plaintiffs and California Class members of the Data Breach.

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

318. California Plaintiffs and California Class members suffered injury in fact and lost money or property as the result of Defendant's unlawful business practices. In addition, California Plaintiffs' and 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. California Plaintiffs and California Class members 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

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

320. Defendant also engaged in unfair business practices under the "tethering test." Defendant's 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."). Defendant's acts and omissions thus amount to a violation of the law.

321. Defendant engaged in unfair business practices under the "FTC test." The harm caused by Defendant's actions and omissions, as described in detail above, is substantial in that it affects thousands of California Class Members and caused those persons to suffer actual harms.

Such harms include a substantial risk of identity theft, disclosure of California Plaintiffs' and 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 California Plaintiffs' and California Class members' PII remains in Defendant's 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).

322. California Plaintiffs and California Class members suffered injury in fact and lost money or property as the result of Defendant's unfair business practices. California Plaintiffs' and 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. California Plaintiffs and California Class members 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.

323. As a result of Defendant's unlawful and unfair business practices in violation of the UCL, California Plaintiffs and California Class members are entitled to damages, injunctive relief, and reasonable attorneys' fees and costs.

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

324. California Plaintiffs incorporate paragraphs 1 through 227 as though fully set forth herein.

325. 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 . . . ."

326. 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).

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

a. The security breach notification shall be written in plain language.

b. The security breach notification shall include, at a minimum, the following information:

i. the name and contact information of the reporting person or business subject to this section;

ii. a list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

iii. if the information is possible to determine at the time the notice is provided, then any of the following:

1. the date of the breach,
2. the estimated date of the breach, or
3. the date range within which the breach occurred. The notification shall also include the date of the notice;
4. 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,
5. a general description of the breach incident, if that information is possible to determine at the time the notice is provided, and
6. 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.

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

329. Defendant failed to disclose to California Plaintiffs and California Class members, without unreasonable delay and in the most expedient time possible, the breach of security of its

unencrypted, or not properly and securely encrypted, PII when Defendant knew or reasonably believed such information had been compromised.

330. Defendant's ongoing business interests gave Defendant incentive to conceal the Data Breach from the public to ensure continued revenue.

331. Upon information and belief, no law enforcement agency instructed Defendant that timely notification to California Plaintiffs and California Class members would impede its investigation.

332. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, California Plaintiffs and 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 California Plaintiffs and California Class members because their stolen information would have had less value to identity thieves.

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

334. California Plaintiffs and California Class members seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to the damages suffered by California Plaintiffs and California Class members as alleged above, and equitable relief.

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 Defendant 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 Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant 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 Defendant to delete, destroy, and purge the PII of Plaintiffs and Class members unless Defendant 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 Defendant to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of Plaintiffs' and Class members' PII;

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

vi. requiring Defendant 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

Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third–party security auditors;

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

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

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

x. requiring Defendant to conduct regular database scanning and security checks;

xi. requiring Defendant 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 Plaintiffs' and Class members' PII;

xii. requiring Defendant 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 Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing

employees' compliance with Defendant's policies, programs, and systems for protecting PII;

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

xv. requiring Defendant to meaningfully educate all Class members about the threats 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 Defendant to design, maintain, and test its computer systems to ensure PII in its possession is adequately secured and protected;

xvii. requiring Defendant to detect and disclose any future data breaches in a timely and accurate manner;

xviii. requiring Defendant to implement multi–factor authentication requirements, if not already implemented;

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

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

e. Awarding Plaintiffs and Class members damages and the members of the California Class statutory 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: November 19, 2021

Respectfully Submitted,

/s/ Gayle M. Blatt
Gayle M. Blatt

/s/ Michael J. Benke
Michael J. Benke

Gayle M. Blatt (*Pro Hac Vice*)
Michael J. Benke (SBN 4947115)
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
gmb@cglaw.com
mbenke@cglaw.com
110 Laurel Street
San Diego, CA 92101
Tel: (619) 238-1811
Fax: (619) 544-9232

Lead Counsel for Plaintiffs and the Class

Rachele R. Byrd (Pro Hac Vice)
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
byrd@whafh.com
750 B Street, Suite 1820
San Diego, California
Tel: (619) 239-4599
Fax: (619) 234-4599

Attorneys for Plaintiffs

Matthew M. Guiney
Lillian Grinnell
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
guiney@whafh.com
grinnell@whafh.com
270 Madison Avenue
New York, NY 10016
Tel: (212) 545-4600;
Fax: (212) 686-0114

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

Karen Wilson-Robinson, Esq.
WILSON & BROWN, PLLC
karen@wilsonbrownlawyers.com
629 Fifth Avenue, Suite 225
Pelham, New York 10803
Telephone: (646) 498-9816

Todd S. Garber Esq.
FINKELSTEIN, BLANKINSHIP,
FREIPEARSON & GARBER, LLP
tgarber@fbfglaw.com
One North Broadway, Suite 900
White Plains, New York 10601
Tel: (914) 298-3281
Fax: (914) 824-1561

Terence R. Coates (Pro Hac Vice)
MARKOVITS, STOCK & DEMARCO, LLC
tcoates@msdlegal.com
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Tel: (513) 651-3700
Fax: (513) 665-0219

Jeffrey S. Goldenberg (Pro Hac Vice)
GOLDENBERG SCHNEIDER, LPA
jgoldenberg@gs-legal.com
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
Tel: (513) 345-8291
Fax: (513) 345-8294

Joseph M. Lyon (Pro Hac Vice)
THE LYON FIRM, LLC
jlyon@thelyonfirm.com
2754 Erie Avenue
Cincinnati, OH 45208
Tel: (513) 381-2333
Fax: (513) 766-9011

Lori G. Feldman (LF-3478)
GEORGE GESTEN MCDONALD PLLC
LFeldman@4-Justice.com
eService@4-Justice.com
102 Half Moon Bay Drive
Croton-on-Hudson, New York 10520
Tel: (917) 983-9321
Fax: (888) 421-4173

David J. George (Pro Hac Vice)
Brittany L. Brown (Pro Hac Vice)
GEORGE GESTEN MCDONALD, PLLC
DGeorge@4-Justice.com
BBrown@4-Justice.com
eService@4-Justice.com
9897 Lake Worth Road, Suite #302
Lake Worth, FL 33467
Tel: (561) 232-6002
Fax: (888) 421-4173

Attorneys for Plaintiffs