UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

CLIFFORD HARRIS, ANDREW KANTACK, and GERALD DAVIS on behalf of themselves and all others similarly situated, **Plaintiffs,** **v.** **USA WASTE-MANAGEMENT RESOURCES, LLC,** **Defendant.**	: : : : : : : :	Case No. 21-cv-1999 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Clifford Harris, Andrew Kantack, and Gerald Davis ("Plaintiffs"), by and through their attorneys, upon personal knowledge as to themselves and their own acts and experiences, and upon information and belief as to all other matters, allege as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this Class Action Complaint ("Complaint") against Defendant USA Waste-Management Resources, LLC ("Waste Management" or "Defendant"), individually and on behalf of all others similarly situated based on Defendant's failure to properly safeguard Waste Management's current and former employees' (and their dependents') personally identifiable information ("PII"), including full names, dates of birth, driver's license numbers, and social security numbers or National IDs.

2. Waste Management 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.

3. On January 21, 2021, Waste Management detected "suspicious activity" on its network. It later determined that between January 21, 2021 and January 23, 2021, an unauthorized party gained access to Waste Management's network and acquired files containing the sensitive PII of Waste Management's current and former employees, as well as their dependents (the "Data Breach"). The Data Breach exposed the PII of more than 268,000 individuals.

4. Inexplicably, Waste Management did not provide notice to victims 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.

5. Waste Management did not adequately safeguard Plaintiffs' PII , and now Plaintiffs and numerous current and former employees (and their dependents) are the victims of a significant data breach that will negatively affect them for the rest of their lives.

6. Waste Management is responsible for allowing this data breach through its failure to implement and maintain reasonable network safeguards, its unreasonable data retention policies, and its failure to comply with industry-standard data security practices.

7. Waste Management had numerous statutory, regulatory, contractual, and common law obligations to keep Plaintiffs' and the Class Members' PII confidential, safe, secure, and protected from unauthorized disclosure or access. For example, in the Waste Management Code of Conduct, Waste Management states: "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 to responsibly collect, store, use, share, transfer and dispose of personally identifiable information."[1]

[1] Waste Management Code of Conduct, April 2021, *available at:* https://sustainability.wm.com/downloads/WM_Code_of_Conduct.pdf (last accessed June 16, 2021).

8. Plaintiffs and those similarly situated relied upon Waste Management to maintain the security and privacy of the PII entrusted to it as part of the condition of employment. Plaintiffs and Class Members reasonably expected and understood that Waste Management would comply with its obligations to keep the information secure and safe from unauthorized access, and to delete PII that was not reasonably necessary to hold for a legitimate business purpose.

9. As a result of Waste Management's failures, Plaintiffs and the Class Members are at a significant risk of identity theft, financial fraud, and/or other identity-theft or fraud, imminently and for years to come.

10. Plaintiffs and members of the proposed Class have suffered actual and imminent injuries as a direct result of the data breach. The 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 and the stress, nuisance and annoyance of dealing with all issues resulting from the data breach; (d) the imminent injury arising from potential fraud and increased risk of identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (e) damages to and diminution in value of their personal data entrusted to Waste Management; (f) the retention of the reasonable value of the PII entrusted to Waste Management; and (g) the continued risk to their personal data which remains in the possession of Waste Management and which is subject to further breaches so long as Waste Management fails to undertake appropriate and adequate measures to protect the PII in its possession.

11. Plaintiffs seek to remedy these injuries, and prevent their future occurrence, on

behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the data breach.

12. Accordingly, Plaintiffs, on behalf of themselves and other members of the Nationwide Class and Employee Sublass (as defined *infra*), assert claims for negligence, implied contract, unjust enrichment, and seeks injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity or by law.

THE PARTIES

Plaintiff Clifford Harris

13. Plaintiff Clifford Harris is a natural person and a resident of Illinois. From 1997 to 2005, Plaintiff Harris was an employee of Defendant Waste Management at the Lombard, Illinois location. In June 2021, Plaintiff Harris received a letter from Waste Management dated May 28, 2021 notifying him that his PII that was provided to Defendant during the course of his employment had been illegally accessed during the Data Breach.[2]

14. Plaintiff Harris entrusted his PII to Waste Management during the course of his employment with the reasonable expectation and understanding that Waste Management would take, at a minimum, industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to him.

15. The letter Plaintiff Harris received dated May 28, 2021, informed him that the PII compromised in the breach included full names, dates of birth, driver's license numbers, and Social Security Numbers or National IDs.

16. The letter offered to provide him with a limited one-year subscription to the credit

[2] A copy of Plaintiff Harris's notice letter from Waste Management is attached as **Exhibit 1**.

monitoring and identity protection service, Experian. However, this purported remedy is insufficient because it does not prevent fraud, but rather monitors for it. Furthermore, the one-year subscription is insufficient as the data included in the breach is permanently compromised, and Plaintiff Harris will remain at risk for identify theft indefinitely. Thus, following the expiration of the one-year subscription, Plaintiff Harris will be forced to pay out of pocket for credit monitoring, which will be necessary for the rest of his life.

17. Since learning about the breach, Plaintiff Harris has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the breach of his PII.

18. Furthermore, Plaintiff Harris has spent time reviewing his financial statements and credit card account information to determine whether there has been any fraudulent activity on his accounts. Plaintiff also intends to take additional steps to place fraud alerts on his credit reports. He will continue to spend additional time every month to review his statements due to the increased risk of identity theft posed by the unlawful disclosure of his PII.

19. Finally, Plaintiff Harris has experienced fraudulent activity on his account that started in February 2021. He has been the victim of three separate incidents where an unauthorized third party has attempted to open a new credit card account in his name. One of the incidents included an attempt to use his information on the "dark web." Following notification of these incidents, Plaintiff Harris had to take time to change his passwords and account information.

Plaintiff Andrew Kantack

20. Plaintiff Andrew Kantack is a natural person and a resident of Florida. Plaintiff Kantack is a former employee of Defendant Waste Management, where he was employed from May 2007 to January 2008 at the Jacksonville, Florida location. In June of 2021, Plaintiff Kantack

received a letter from Waste Management dated May 28, 2021, notifying him that the PII he provided to Defendant during the course of his employment had been accessed during the Data Breach.[3]

21. Plaintiff Kantack entrusted his PII to Waste Management with the reasonable expectation and understanding that Waste Management would take, at a minimum, industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to him.

22. The letter Plaintiff Kantack received dated May 28, 2021, informed him that the PII compromised in the breach included full names, dates of birth, driver's license numbers, and Social Security Numbers or National IDs.

23. The letters offered to provide him with a limited one-year subscription to the credit monitoring and identity protection service, Experian. However, this purported remedy is insufficient because it does not prevent fraud, but rather monitors for it. Furthermore, the one-year subscription is insufficient as the data included in the breach is permanently compromised, and Plaintiff Kantack will remain at risk for identity theft indefinitely. Thus, following the expiration of the one-year subscription, Plaintiff Kantack will be forced to pay out of pocket for credit monitoring, which will be necessary the rest of his life.

24. Since learning about the breach, Plaintiff Kantack has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the breach of his PII.

25. Furthermore, Plaintiff Kantack has spent approximately 40 hours reviewing his personal information and accounts after learning of the Data Breach. This time has included

[3] A copy of Plaintiff Kantack's notice letter from Waste Management is attached as **Exhibit 2**.

reviewing his financial statements and credit card account information to determine whether there has been any fraudulent activity on these accounts, and Plaintiff Kantack has taken additional steps to place fraud alerts on his credit reports and monitoring services, changing passwords, signing up for new monitoring services, and ordering a new credit card. He will continue to take additional time every month to review his statements due to the increased risk of identity theft posed by the unlawful disclosure of his PII.

Plaintiff Gerald Davis

26. Plaintiff Gerald Davis is a natural person and a resident of Indiana. Plaintiff is a former employee of Defendant Waste Management, where he was employed from August 2010 to December 2012 at the Louisville, Kentucky location. In June of 2021, Plaintiff Davis received a letter from Waste Management dated May 28, 2021 notifying him that the PII he provided during the course of his employment had been accessed during the Data Breach.[4]

27. Plaintiff Davis entrusted his PII to Waste Management with the reasonable expectation and understanding that Waste Management would take, at a minimum, industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to him.

28. The letter Plaintiff Davis received dated May 28, 2021, informed him that the PII compromised in the breach included full names, dates of birth, driver's license numbers, and Social Security Numbers or National IDs.

29. The letters offered to provide him with a limited one-year subscription to the credit monitoring and identity protection service, Experian. However, this purported remedy is insufficient because it does not prevent fraud, but rather monitors for it. Furthermore, the one-year

[4] A copy of Plaintiff Davis's notice letter from Waste Management is attached as **Exhibit 3**.

subscription is insufficient as the data included in the breach is permanently compromised, and Plaintiff Davis will remain at risk for identity theft indefinitely. Thus, following the expiration of the one-year subscription, Plaintiff Davis will be forced to pay out of pocket for credit monitoring, which will be necessary the rest of his life.

30. Since learning about the breach, Plaintiff Davis has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the breach of his PII.

31. Furthermore, Plaintiff Davis has spent time reviewing his financial statements and account information to determine whether there has been any fraudulent activity on his accounts. He has also taken additional steps to place fraud alerts on his credit reports. He will continue to take additional time every month to review his statements due to the increased risk of identity theft posed by the unlawful disclosure of his PII.

Defendant Waste Management

32. Waste Management is a limited liability company organized under the laws of New Jersey and headquartered with its principal place of business located in Houston, Texas. Upon information and belief, Waste Management is a wholly owned subsidiary of the publicly traded corporation, Waste Management, Inc. Service of process is proper on Waste Management at 800 Capital Street, Suite 3000, Houston, Texas 77002.

JURISDICTION & VENUE

33. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d)(2), as modified by the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1711, *et seq.*, because at least one member of the Class, as defined below, is a citizen of a different state than Waste Management, there are more than 100 putative Class Members and the amount in controversy

exceeds $5,000,000, exclusive of interest and costs.

34. This Court has general personal jurisdiction over Waste Management because Waste Management's principal place of business is in Houston, Texas.

35. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, and Defendant conducts substantial business in this District.

FACTUAL ALLEGATIONS

36. Waste Management offers a wide range of services including solid waste and recyclable materials collection services for residential, industrial, municipal and commercial customers in 48 states. It serves over 20 million residential customers and over 2 million commercial customers.

37. Waste Management currently has in excess of 48,000 full-time employees.

38. Waste Management requires its employees to provide sensitive PII as a condition of employment. Waste Management's employees are also required to provide the PII of their dependents.

The Data Breach

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

40. Waste Management later determined that between January 21, 2021 and January 23, 2021, an unauthorized actor(s) accessed Waste Management's network and acquired certain files containing the sensitive PII of Waste Management's current and former employees.

41. As of the date of filing of this Complaint, the PII of more than 268,000 individuals was exposed in the breach. These individuals include Waste Management's current and former

employees, as well as the dependents of certain current and former employees. Impacted Plaintiffs and current and former employees worked at Waste Management facilities throughout the country.

42. The unauthorized actor(s) were able to gain access to Waste Management's network as a result of Waste Management's failure to take necessary and required minimal steps to secure Plaintiffs' and the Class Members' PII. Similarly, Waste Management's failure to take reasonable steps after detecting suspicious activity on January 21, 2021 allowed the criminal third party actor(s) to maintain access to Waste Management's network on January 22 and 23, 2021.

43. Despite first detecting "suspicious activity" on January 21, 2021, Waste Management did not begin notifying victims of the breach until May 28, 2021. A copy of a sample notice letter filed with the California Attorney General is attached hereto as **Exhibit 4**.

44. The notice letters offer victims of the breach one free year of credit and identity monitoring services through Experian.

Plaintiffs and the Class Have Been Injured and Face Substantial Risk of Future Injury

45. Plaintiffs' and Class Members' stolen personal data represents essentially one-stop shopping for identity thieves. The unauthorized access by the hackers has provided cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential PII to mimic the identity of the user.

46. Criminals often trade stolen PII on the "cyber black market" for years following a breach. Cybercriminals can also post stolen PII on the internet, thereby making such information publicly available.

47. The ramifications of Waste Management'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.

48. 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.[5] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[6]

49. 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.

50. Recently, the FTC has released its updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

51. The FTC has, upon information and belief, brought enforcement actions against businesses for failing to protect PII. The FTC has done this by treating a failure to employ

[5] *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 June 17, 2021).

[6] https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft. 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*.

reasonable measures to protect against unauthorized access to PII as a violation of the FTC Act, 15 U.S.C. § 45.

52. 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.[7]

53. Waste Management 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. Waste Management failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

54. Plaintiffs and the Class Members are at constant risk of imminent and future fraud, identity theft, and misuse of their PII for many years in the future as a result of the Defendant's actions and the Data Breach. They have suffered real and tangible loss, including but not limited to the loss in the inherent value of their PII, the loss of their time as they have had to spend additional time monitoring accounts and activity, and additional economic loss to mitigate the costs of injuries realized as a result of the breach.

Defendant Acknowledges the Impact of this Data Breach on Plaintiffs and the Class

55. It is common sense that the criminals who breached Waste Management's systems and acquired the victims' PII did so for the purpose of using that data to commit fraud, theft, and other crimes, or for the purpose of the selling or providing the PII to other individuals intending to

[7] *See* https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07-737/html/GAOREPORTS-GAO-07-737.htm (last visited June 17, 2021).

commit fraud, theft, and other crimes. Given that this is the reason such PII is sought by criminals, it is similarly common sense that Plaintiffs and the Class Members have already suffered injury and face a substantial risk for imminent future injury.

56. Waste Management acknowledges the risk faced by victims of the breach. This is evidenced by Waste Management's extension of one year of credit and identity monitoring services to victims of the breach. It is common sense that Waste Management would not spend money procuring such services for victims of the Data Breach if such victims were not harmed and/or did not face a substantial risk of imminent harm.

57. Similarly, Waste Management's notice letter implicitly acknowledges harm faced by Data Breach victims by stating: "We also encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your free credit reports for suspicious activity."

58. Furthermore, the notification letters sent to Plaintiffs and Class Members include a document titled "STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION." In addition to the information discussed above, this document informs victims that they may wish to place initial or extended fraud alerts on credit files or obtain a credit freeze by contacting each of the three major credit reporting bureaus.

59. Waste Management acknowledges that victims following the advice to obtain a credit freeze will be further inconvenienced and harmed as a result of taking these reasonable steps to prevent future harm. Specifically, it states that "you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of

credit."

The Value of Private Information and Effects of Unauthorized Disclosure

60. Waste Management knew or should have known that the protected PII it acquires is highly sensitive and of significant value to those who would use it for wrongful purposes.

61. PII is a valuable commodity to identity thieves, particularly when it is aggregated in large numbers and when multiple types of information for a single user are combined. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical or financial fraud.[8] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and other protected financial information on multiple underground Internet websites, commonly referred to as the "dark web."

62. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[9]

63. Individuals 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.

64. PII has been valued on the dark web at approximately $1 per line of information.[10]

65. One study on website privacy determined that U.S. consumers valued the restriction

[8] https://www.identitytheft.gov/warning-signs-of-identity-theft (last visited on June 17, 2021).
[9] FEDERAL TRADE COMMISSION, *The Information Marketplace: Merging and Exchanging Consumer Data*, *transcript available* at http://www.ftc.gov/news-events/events-calendar/2001/03/information-marketplace-merging-exchanging-consumer-data (last visited June 17, 2021).
[10] https://www.pacetechnical.com/much-identity-worth-black-market/#:~:text=Personally%20identifiable%20information%20is%20sold,at%20a%20fast%20food%20joint. (last visited on June 17, 2021).

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."[11] 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.

66. Beside the monetary damage sustained, consumers may also spend anywhere from approximately 7 hours to upwards to over 1,000 hours trying to resolve identity theft issues.[12]

The Sort of PII at Issue Here is Particularly Valuable to Hackers

67. Credit card and bank account numbers are tempting targets for hackers. However, information like dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

68. The unauthorized disclosure of Social Security numbers can be particularly damaging, because Social Security numbers cannot easily be replaced. In order to obtain a new Social Security number a person must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, no new Social Security number can be obtained until the damage has been done.

69. Furthermore, as the Social Security Administration ("SSA") warns:

> 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)

[11] 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 June 17, 2021).
[12] https://www.lifelock.com/learn-identity-theft-resources-how-long-does-it-take-to-recover-from-identity -theft.html #:~:text=And%20ID%20theft%20recovery%20is,more%20resolving%20identity%20theft%20problems. (last visted on June 17, 2021).

> 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.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> 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.[13]

70. Criminals can, for example, use Social Security numbers to create false bank accounts, open credit card accounts, or file fraudulent tax returns.[14] Former and current Waste Management employees (as well as their dependents) whose Social Security numbers have been compromised will and already have spent time contacting various agencies, such as the Internal Revenue Service and the Social Security Administration. They also now face a real and imminent substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

71. Again, because the information Defendant allowed to be compromised and taken is of such a durable and near-permanent quality, the harms to Plaintiffs and the Class will continue to grow, and Plaintiffs and the Class will continue to be at substantial risk for further imminent and future harm.

72. As a result of Waste Management's failure to prevent the Data Breach, Plaintiffs and Class Members have suffered and will continue to suffer injuries, including loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the

[13] 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 June 17, 2021).

[14] When fraudulent tax returns are filed, the requirements for a legitimate taxpayer to file their tax returns with the IRS increase, including the necessity to obtain and utilize unique PIN numbers just to be able to file a tax return.

Data Breach; theft of their valuable PII; the imminent and certainly impending injury flowing from fraud and identity theft posed by their PII being placed in the hands of criminals; damages to and diminution in value of their PII that was entrusted to Defendant with the understanding the Defendant would safeguard the PII against disclosure; and continued risk to Plaintiffs' and the Class Members' PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to it.

Data Breaches Have Become More Prevalent

73. The frequency of cyberattacks has increased significantly in recent years.[15]

74. 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."[16]

75. 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."[17]

[15] *See* https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50 (last visited June 17, 2021).
[16] https://www.isaca.org/resources/news-and-trends/industry-news/2020/top-cyberattacks-of-2020-and-how-to-build-cyberresiliency (last visited June 17, 2021) (citing Cybersecurity Ventures, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016).
[17] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016 (last visited June 17, 2021).

76. As noted in recent reports by Deloitte and Interpol, cyberattacks have greatly increased in the wake of the COVID-19 pandemic.[18]

Defendant Had a Duty to Protect Plaintiffs' and Class Members' PII

77. Waste Management knew or should have known it was and continues to be an ideal target for cyberattacks. This is based on Waste Management's knowledge of information such as its own failure to take reasonable steps to maintain the security of its data, the value of the PII it stored, the quantity of PII it stored, and the prevalence of data breaches in recent years.

78. By requiring the production of, collecting, obtaining, using, and deriving benefits from Plaintiffs' and the Class Members' PII, Waste Management assumed certain legal and equitable duties and knew or should have known that it was responsible for the diligent protection of the PII it collected and stored.

79. As a wholly owned subsidiary of a highly successful publicly traded company with a market capitalization of roughly $50 billion, Waste Management had the resources to invest in the necessary data security and protection measures. Yet, it failed to undertake adequate analyses and testing of its own systems, adequate personnel training, and other data security measures to avoid the failures that resulted in the Data Breach.

80. Waste Management is aware of the importance of security in maintaining personal information, and the value individuals place on keeping their PII secure.

81. Realizing its duty with respect to PII, the notification letters sent to Class Members acknowledge the importance of data security and Waste Management's duty to the Class Members, stating that Waste Management "take[s] the confidentiality, privacy, and security of information

[18] https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html (last visited June 17, 2021); https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats (last visited June 17, 2021).

in [its] care seriously."

82. Despite its awareness, Waste Management did not take the necessary and required minimal steps to secure Plaintiffs' and the Class Members' PII. As a result, hackers breached and stole important PII from at least hundreds of thousands of Waste Management's current and former employees, as well as their dependents.

83. Defendant owes a further duty to its employees (and their dependents) to immediately and accurately notify them of a breach of its systems to protect them from identity theft and other misuse of their personal data and to take adequate measures to prevent further breaches.

Defendant's Post-Breach Activity was Inadequate

84. Immediate notice of a security breach is essential to protect people such as Plaintiffs and the Class Members. Defendant failed to provide such immediate notice, in fact taking roughly four months to disclose to Plaintiffs and the Class Members that there had been a breach, thus further exacerbating the damages sustained by Plaintiffs and the Class resulting from the breach.

CLASS ACTION ALLEGATIONS

85. 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 Class defined below.

86. Under Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action as a national Class action for themselves and all members of the following Class of similarly situated persons:

The Nationwide Class

> All natural persons residing in the United States whose personal information was compromised in the Waste Management Data Breach, which occurred between

approximately January 21, 2021 and January 23, 2021.[19]

87. Plaintiffs also bring this action on behalf of the following Subclass of similarly siuated persons:

The Employee Subclass

> All natural persons residing in the United States and currently or formerly employed by Waste Management whose personal information was compromised in the Waste Management Data Breach, which occurred between approximately January 21, 2021 and January 23, 2021.

88. The Nationwide Class and Subclass may be referred to collectively, where appropriate, as the "Class."

89. Excluded from the Class are Defendant; any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judges and court personnel in this case and any members of their immediate families.

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

91. Certification of Plaintiffs' claims for Class-wide treatment is appropriate because Plaintiffs can prove the elements of the claims on a Class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

92. All members of the proposed Class are readily ascertainable in that Waste Management has access to addresses and other contact information for all members of the Class, which can be used to provide notice to Class Members.

[19] Plaintiffs reserve the right to amend this proposed class definition in the future.

93. ***Numerosity***. The Class and Subclass are so numerous that joinder of all members is impracticable. The Nationwide Class includes at least hundreds of thousands of individuals whose personal data was entrusted to Waste Management and compromised in the Waste Management Data Breach.

94. Upon information and belief, the Subclass includes at least hundreds of individuals whose personal data was entrusted to Waste Management and compromised in the Waste Management Data Breach.

95. ***Commonality***. There are numerous questions of law and fact common to Plaintiffs and the Class, including the following:

- whether Defendant engaged in the wrongful conduct alleged in this Complaint;
- whether Defendant's conduct was unlawful;
- whether Defendant failed to implement and maintain reasonable systems and security procedures and practices to protect PII;
- whether Defendant unreasonably delayed in notifying those affected of the security breach;
- whether Defendant owed a duty to Plaintiffs and Class Members to adequately protect their PII and to provide timely and accurate notice of the Waste Management Data Breach to Plaintiffs and Class Members ;
- whether Defendant breached its duties to protect the PII of Plaintiffs and Class Members by failing to provide adequate data security and failing to provide timely and adequate notice of the Waste Management Data Breach to Plaintiffs and the Class Members;
- whether Defendant's conduct was negligent;
- whether Defendant wrongfully or unlawfully failed to inform Plaintiffs and Class Members that it did not ensure that networks and security practices adequate to reasonably protect PII were used when handling Plaintiffs' and the Class Members' PII;
- whether Defendant should have notified the public, Plaintiffs, and Class Members immediately upon learning of the Data Breach;

- whether Plaintiffs and Class Members suffered injury, including ascertainable losses, as a result of Defendant's conduct (or failure to act);
- whether Plaintiffs and Class Members are entitled to recover damages; and,
- whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

96. ***Typicality***. Plaintiffs' claims are typical of the claims of the Class in that Plaintiffs, like all Class Members, had their personal data compromised, breached and stolen in the Waste Management security breach. Plaintiffs and all Class Members were injured through Defendant's uniform misconduct described in this Complaint and assert the same claims for relief.

97. ***Adequacy***. Plaintiffs and counsel will fairly and adequately protect the interests of the Class. Plaintiffs has retained counsel who are experienced in Class action and complex litigation. Plaintiffs have no interests that are antagonistic to, or in conflict with, the interests of other members of the Class.

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

99. ***Superiority***. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiffs and Class Members have been injured by Defendant's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct and/or inaction. Plaintiffs know of no difficulties that would be encountered in this litigation that would preclude its maintenance as a

class action.

100. 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.

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

COUNT I
NEGLIGENCE
(on behalf of the Nationwide Class)

102. Plaintiffs restate and reallege all proceeding allegations above and hereafter as if fully set forth herein.

103. Waste Management owed a duty to Plaintiffs and Class Members to safeguard their sensitive PII.

104. As their employer, Waste Management also had a special relationship with its current and former employees from being entrusted with their PII (and the PII of their dependents), which provided an independent duty of care.

105. Waste Management had a duty to use reasonable security measures because it undertook to collect, store and use Plaintiffs and Class members' personal information.

106. As part of this duty, Waste Management was required to implement adequate data

security safeguards and measures to prevent foreseeable injury to Plaintiffs and the Class Members, and therefore had a duty to take reasonable steps to safeguard sensitive PII from unauthorized release or theft.

107. A network or system security breach by a third party criminal enterprise was a foreseeable risk that Waste Management knew or should have known could damage its employees and their dependents and expose them to the risk of identify theft.

108. In other words, Waste Management was required to exercise reasonable care in obtaining, retaining, securing, storing, safeguarding, deleting and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

109. Waste Management's duty included, among other things, designing, maintaining, and testing its security systems and data retention policies to ensure that Plaintiffs' and Class members' PII in its possession was adequately secured, protected, and safely deleted in a timely manner.

110. Waste Management further owed a duty to Plaintiffs and Class Members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts.

111. There is a very close connection between Waste Management's failure to follow reasonable security standards to protect the PII and the injury to Plaintiffs and the Class Members. When individuals have their PII stolen, they are at substantial risk for imminent identity theft, and need to take steps to protect themselves, including, for example, buying credit monitoring services and purchasing or obtaining credit reports to protect themselves from identity theft.

112. If Waste Management had taken reasonable security and data retention measures, data thieves would not have been able to take the PII of Plaintiffs and the Class Members. The

policy of preventing future harm weighs in favor of finding a special relationship between Waste Management and Plaintiffs and the Class. If companies are not held accountable for failing to take reasonable security measures to protect PII in their possession, they will not take the steps that are necessary to protect against future security breaches.

113. Waste Management breached its duties by the conduct alleged in the Complaint by, including without limitation, failing to protect the PII in its possession; unreasonably retaining plaintiffs PII; failing to maintain adequate computer systems and data security practices to safeguard the PII in its possession; failing to utilize adequate, updated, and secure software and related systems to protect the PII in its possession; failing to disclose the material fact that its computer systems and data security practices were inadequate to safeguard the PII from theft; and failing to disclose in a timely and accurate manner to Plaintiffs and Class Members the material fact of the Data Breach.

114. As a direct and proximate result of Waste Management's failure to exercise reasonable care and use commercially reasonable security measures, the PII of Waste Management's employees (and their dependents) was accessed by ill-intentioned criminals who have used and will use the information to commit identity or financial fraud. Plaintiffs and Class Members face the imminent, certainly impending and substantially heightened risk of identity theft, fraud and further misuse of their PII.

115. As a proximate result of this conduct, Plaintiffs and the Class Members suffered damage after the unauthorized data release and will continue to suffer damages in an amount to be proven at trial. Furthermore, Plaintiffs and the Class Members have suffered emotional distress as a result of the breach and have lost time and/or money as a result of past and continued efforts to protect their PII and prevent the unauthorized use of their PII.

COUNT II
DECLARATORY JUDGMENT
(on behalf of the Nationwide Class)

116. Plaintiffs restate and reallege all proceeding allegations above and hereafter as if fully set forth herein.

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

118. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII and whether Waste Management is currently maintaining data security measures adequate to protect Plaintiffs' and Class Members from further data breaches that compromise their PII. Plaintiffs allege that Waste Management's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

119. Under its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Waste Management owes a legal duty to secure PII and to timely notify victims of a data breach under the common law; and

b. Waste Management continues to breach this legal duty by failing to employ reasonable measures to secure individuals' PII.

120. This Court also should issue corresponding prospective injunctive relief requiring Waste Management to employ adequate security protocols consistent with law and industry standards to protect PII.

121. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Waste Management. The risk of another such breach is real, immediate, and substantial. If another breach at Waste Management occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

122. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Waste Management if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Waste Management of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Waste Management has a pre-existing legal obligation to employ such measures.

123. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Waste Management, thus eliminating the additional injuries that would result to Plaintiffs and individuals whose Payment Information would be further compromised.

COUNT III
BREACH OF IMPLIED CONTRACT
(on behalf of the Employee Subclass)

124. Plaintiffs restate and reallege all proceeding allegations above and hereafter as if fully set forth herein.

125. Plaintiffs and the Employee Subclass members delivered their PII to Waste

Management as part of the process of obtaining employment and/or services provided by Waste Management.

126. Plaintiffs and Employee Subclass members entered into implied contracts with Waste Management under which Plaintiffs and Employee Subclass members agreed to provide PII as terms of the employment and Waste Management agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Employee Subclass members that their data had been breached and compromised.

127. Plaintiffs and putative members of the Employee subclass entered into implied contracts with Waste Management under which Waste Management agreed to only retain such PII for a reasonable amount of time and for legitimate business purpose.

128. In providing such data, Plaintiffs and the Employee Subclass members entered into an implied contract with Waste Management whereby Waste Management became obligated to reasonably safeguard Plaintiffs' and the other Class Members' PII. Defendant's obligations to protect the data added value to the employment relationship and implied contract.

129. In delivering their PII to Waste Management, Plaintiffs and Employee Subclass members intended and understood that Waste Management would adequately safeguard their personal data.

130. Plaintiffs and the Employee Subclass members would not have entrusted their PII to Waste Management in the absence of such an implied contract.

131. Waste Management accepted possession of Plaintiffs' and Employee Subclass members' PII for the purpose of providing employment and/or services to Plaintiffs and Employee Subclass members.

132. Had Waste Management disclosed to Plaintiffs and Employee Subclass members

that it would maintain their PII for long periods, including several decades after their employment with Waste Management, and would fail to adequately protect Plaintiffs' and the Employee Subclass members' PII, Plaintiffs and Employee Subclass members would not have provided their PII to Waste Management.

133. Waste Management knew that its employees' personal data is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and Employee Subclass members.

134. Plaintiffs and Employee Subclass members fully performed their obligations under the implied contracts with Waste Management.

135. Waste Management breached the implied contract with Plaintiffs and the Employee Subclass members by failing to take reasonable measures to safeguard their PII.

136. Waste Management's breach of the implied contract created a loss of value as Plaintiffs and Employee Subclass members did not receive the full benefit of the bargain of the implied contract.

137. As a proximate result of Defendant's conduct, Plaintiffs and the Employee Subclass members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT IV
UNJUST ENRICHMENT
(on behalf of the Employee Subclass)

138. Plaintiffs incorporate by reference all other allegations in the Complaint as if fully set forth herein.

139. Plaintiffs and Employee Subclass members conferred a benefit on Waste Management by working for and performing services to Waste Management. Waste Management had knowledge of this benefit when it employed Plaintiffs and the Employee Subclass members

and accepted their work and services.

140. In exchange for the work and services performed by Plaintiffs and Employee Subclass members to the benefit of Waste Management, Waste Management should have, in part, provided for the administrative and other costs of providing reasonable data security and protection to Plaintiffs and Employee Subclass members.

141. Waste Management failed to provide reasonable security, safeguards, and protections to the personal data of Plaintiffs and Employee Subclass members, instead permitting unauthorized third parties access to Plaintiffs' and Employee Subclass members' PII.

142. Furthermore, Waster Management retained valuable PII for long periods of time without any consideration provided to Plaintiffs and Employee Subclass members for the retention of the PII.

143. Under principles of equity and good conscience, Waste Management should not be permitted to retain the benefit of work, services, and the PII that Plaintiffs and Employee Subclass members bestowed upon Waste Management because Waste Management failed to provide adequate safeguards and security measures to protect Plaintiffs' and Employee Subclass members' PII.

144. Waste Management wrongfully accepted and retained these benefits to the detriment of Plaintiffs and Employee Subclass members .

145. Waste Management's enrichment at the expense of Plaintiffs and Employee Subclass members is and was unjust.

146. As a result of Waste Management's wrongful conduct, as alleged above, Plaintiffs and the Employee Subclass members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Waste Management, plus attorneys' fees, costs, and

interest thereon.

RELIEF REQUESTED

Plaintiffs, individually and on behalf of the proposed Class, request that the Court:

1. Certify this case as a Class action on behalf of the Class defined above, appoint Plaintiffs as Class representative, and appoint the undersigned counsel as Class counsel;

2. Award declaratory, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and other Class Members;

3. Award restitution and damages to Plaintiffs and Class Members in an amount to be determined at trial;

4. Award Plaintiffs and Class Members their reasonable litigation expenses and attorneys' fees to the extent allowed by law;

5. Award Plaintiffs and Class Members pre- and post-judgment interest, to the extent allowable; and,

6. Award such other and further relief as equity and justice may require.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of any and all issues in this action so triable of right.

Respectfully submitted,

/s/ William R.H. Merrill
William R.H. Merrill
Texas Bar No. 24006064
S.D. Admission No. 23601
SUSMAN GODFREY, L.L.P.
1000 Louisiana
Houston, TX 77002
Phone: (713) 653-7865
Fax: (713) 654-6666
bmerrill@susmangodfrey.com

Krysta Kauble Pachman
(*Pro Hac Vice Forthcoming*)
SUSMAN GODFREY, L.L.P.
1900 Avenue of the Stars
Los Angeles, CA 90067

Phone: (310) 789-3118
Fax: (310) 789-3150
kpachman@susmangodfrey.com

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

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

Joseph M. Lyon (*pro hac vice forthcoming*)
THE LYON FIRM
2754 Erie Avenue
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

Counsel for Plaintiffs and the Proposed Class