Thomas V. Girardi, (SBN: 36603)
tgirardi@girardikeese.com
Keith D. Griffin, (SBN: 204388)
kgriffin@girardikeese.com
GIRARDI | KEESE
1126 Wilshire Boulevard
Los Angeles, California 90017
Telephone: (213) 977-0211
Facsimile: (213) 481-1554

Jad Sheikali (*pro hac vice*)
jsheikali@mcgpc.com
David L. Gerbie (*pro hac vice*)
dgerbie@mcgpc.com
MCGUIRE LAW, P.C.
55 West Wacker Drive, 9th Floor
Chicago, Illinois 60601
Telephone: (312) 893-7002
Facsimile: (312) 275-7895

Ebby S. Bakhtiar (SBN: 215032)
esb@livingstonbakhtiar.com
LIVINGSTON • BAKHTIAR.
3435 Wilshire Boulevard, Suite 1669
Los Angeles, CA 90010
Telephone: (213) 632-1550
Facsimile: (213) 632-3100

Attorneys for Plaintiffs and the Putative Class

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

EVELIA DAVILA, individually and on behalf of similarly situated individuals,

Plaintiff,

v.

ABM INDUSTRIES, INC., a Delaware Corporation; AMERICAN BUILDING MAINTENANCE CO., a Business Entity Form Unknown; ABM ONSITE SERVICES WEST, INC., a Delaware Corporation; ABM SERVICES, INC., a Business Entity Form Unknown, and DOES 1 through 100, inclusive,

Defendants.

CASE No.: 2:18-CV-03919 FMO (Ex)

PLAINTIFFS' SECOND AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

1. NEGLIGENCE
2. VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW CAL. BUS. & PROF. CODE § 17200 - UNLAWFUL BUSINESS PRACTICES
3. VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW CAL. BUS. & PROF. CODE §17200 UNFAIR BUSINESS PRACTICES
4. VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW CAL. BUS. & PROF. CODE §17200 FRAUDULENT/DECEPTIVE BUSINESS PRACTICES
5. CONSTITUTIONAL INVASION OF PRIVACY

LARRY WADE, individually and on behalf similarly situated individuals,

Plaintiff,

v.

ABM INDUSTRIES INCORPORATED, a Delaware Corporation,

Defendant.

6. NEGLIGENCE *PER SE*
7. VIOLATION OF STATE DATA BREACH ACTS
8. VIOLATION OF N.Y. GENERAL BUSINESS LAW § 349, *ET SEQ.*
9. BREACH OF CONTRACT
10. BREACH OF IMPLIED CONTRACT
11. VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT 815 ILCS 505/1, *ET SEQ.*
12. VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT.

JURY TRIAL DEMANDED

PLAINTIFFS' SECOND AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs EVELIA DAVILA and LARRY WADE (together, the "Plaintiffs"), both individually and on behalf of all others similarly situated (the "Class," "California Subclass," and "Illinois Subclass," as defined below), through their undersigned counsel, hereby allege the following based upon information and belief formed by investigation made by their attorneys, except those allegations relating to Plaintiffs and their attorneys, which are based on knowledge:

NATURE OF THE ACTION

1. Defendants ABM INDUSTRIES, INC., AMERICAN BUILDING MAINTENANCE CO., ABM ONSITE SERVICES WEST, INC., ABM SERVICES, INC. as well as DOES 1 to 100 (collectively, "ABM" or "Defendants"), on information and belief, were and are corporations or business entities conducting business in the County of Los Angeles.

2. Between June 1999 and May 2010, Plaintiff Davila worked for ABM as a member of a cleaning crew. During her decade of employment with ABM, Plaintiff Davila regularly worked nights and consistently performed her job duties to ABM's satisfaction. Plaintiff Larry Wade was at all relevant times employed by Defendants in Illinois through early 2018.

3. Plaintiffs, both individually and on behalf of the Class, bring this action to secure redress against ABM for their reckless and negligent violations of the Class members' privacy rights. Plaintiffs and the Class members are current or former ABM employees who entrusted ABM with their personal, financial, and other confidential information. During Plaintiffs' employment, they entrusted ABM with their full name, Social Security number, birth date, address(es), driver's license number, credit card numbers, medical information (including biometric information), and other highly-sensitive information (collectively, "Private Identifiable Information" or "PII").

4. On or around March 12, 2018, Plaintiffs were informed by ABM that, as of August 1, 2017, ABM knew that ABM had suffered a data breach (the "2017 Data Breach") that allowed third parties to access Plaintiffs' and Class members' PII. Plaintiffs were informed that third parties obtained their PII through a "phishing" attack, where unauthorized individuals infiltrate unsecure networks by sending malware through email servers to obtain valuable information, install dangerous software, and/or accomplish other nefarious objectives.

5. Additionally, since the Data Breach, ABM suffered a second data breach (the "2018 Data Breach") between January 8, 2018, and August 7, 2018, affecting approximately 60,000 ABM employees, including Plaintiff Wade. The 2018 Data Breach, like the 2017 Data Breach (collectively, the "Data Breaches"), was caused by a phishing attack.

6. ABM's conduct was negligent and reckless in allowing third parties to gain access to Plaintiffs' and Class members' PII. On information and belief, the PII obtained in the attack has compromised Class members' identities.

7. Plaintiffs and Class members suffered both pecuniary and non-pecuniary injury as a result of the Data Breaches, including their PII being compromised.

8. Due to ABM's wrongful actions and inactions, Plaintiffs' and Class members' PII was stolen and misappropriated, exposing them to fraud, identify theft, and other concrete harms.

PARTIES

9. At all times relevant to this action, Plaintiff Davila is and was a resident of Los Angeles County in the state of California. At all times relevant to this action, Plaintiff Wade is and was a resident of Cook County in the state of Illinois.

10. Plaintiffs bring this action individually and on behalf of all others who similarly entrusted ABM with their PII. Upon information and belief, Defendants are Delaware corporations, or business entities of unknown form, doing substantial business in California and Illinois with one of their California addresses listed as 1150 S. Olive Street, Suite 1900, Los Angeles, California 90015. Defendants are headquartered in New York.

11. The true names and/or capacities, whether individual, corporate, associate or otherwise, of Defendants Does 1 through 100 (the "Does"), inclusive, and each of them, are unknown to Plaintiffs, who therefore sue said Does by such fictitious names. Plaintiffs are informed and believe, and upon such information and belief allege, that each of the Does fictitiously named herein is legally responsible, negligently or in some other actionable manner, for the events and happenings hereinafter referred to, and proximately caused the injuries and damages to Plaintiffs hereinafter alleged. Plaintiffs will seek leave of Court to amend this Complaint to assert the true names and/or capacities of such fictitiously named Does when the same have been ascertained.

12. Plaintiffs are informed and believe, and thereupon allege, that at all times mentioned herein, Defendants, and each of them, including the Does, were the agents, servants, employees and/or joint ventures of their co-Defendants.

JURISDICTION AND VENUE

13. This Court has diversity jurisdiction under 28 U.S.C. § 1332(d), because (i) at least one member of the putative class is a citizen of a state different from any Defendants, (ii) the amount in controversy exceeds $5,000,000 exclusive of interests and costs, and (iii) none of the exceptions under that subsection apply to the instant action.

14. This Court has personal jurisdiction over Defendants because Defendants transact business in California and because a substantial part of the events giving rise to Plaintiffs' claims arise out of Defendants' unlawful in-state actions. Further, ABM employs thousands of individuals in California. Thus, this Court has personal jurisdiction over Defendants because they have sufficient minimum contacts with California and because Defendants have consented to the jurisdiction of this Court.

15. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to Plaintiffs' claims occurred in this District. Venue is also proper because ABM have consented to the jurisdiction of this Court.

SUBSTANTIVE ALLEGATIONS

A. *The Data Breach Unravels*

16. ABM maintain PII of their current and former employees.

17. On or around August 1, 2017, ABM discovered that they had been the target of a major and successful cybersecurity breach that resulted in the unauthorized disclosure of the PII of thousands of their employees.

18. Despite learning of the breach in or about August 2017, ABM waited until March 2018, over seven months later, to inform affected persons, including Plaintiffs, of the breach.

19. There was no legitimate reason for ABM to wait so long to inform Plaintiffs and Class members that their PII had been compromised. Further, this is not the first time that ABM have been targeted by a cyber-attack. In 2011, ABM were the target of a cyber-attack on their Information Technology ("IT") systems, where many ABM employees' PII ended up in the hands of criminal(s). Despite this clear warning and awareness of the risk of future such cyber-attacks, on information and belief, ABM took insufficient steps to improve the security of their IT systems. The Data Breaches, which are the subject of the present action, occurred several years later and were reasonably foreseeable.

20. By virtue of the 2011 cyber-attack, as well as basic industry knowledge regarding cybersecurity best practices, ABM were not only aware of the risks associated with unauthorized exposure of PII, but, notably, the importance of taking prompt measures to notify affected parties and mitigate identity theft.

21. Plaintiffs and Class members trusted ABM with their PII. Had Defendants informed Plaintiffs and Class members of the Data Breaches within a reasonable period, as required by law, they would have been able to take actions to protect their identities, financial accounts, and other targets from further hacking attempts. Further, Plaintiffs either would have not entered into an employment relationship with ABM, or would have demanded higher compensation in exchange,

had they been aware of the risk that ABM would leave their PII vulnerable to attack. Instead, Defendants failed to properly secure their employees' sensitive information and then let their employees languish in ignorance as to the real risk of irreversible privacy harms presented by the unauthorized parties who had gained access to their PII.

22. Plaintiffs' and Class members' PII has been compromised through ABM's negligent and reckless actions. ABM did not inform Plaintiffs of when the attack actually occurred, but only when ABM "discovered" the attack, which was seven months prior to the date of notification to the Class members. Therefore, it may have been even longer than seven months between when the 2017 Data Breach occurred and when Plaintiffs and Class members were first informed.

23. Further, on March 11, 2019, Plaintiff Wade was notified that his PII was exposed in the 2018 Data Breach, another phishing attack that occurred between January 8, 2018, and August 7, 2018. Plaintiff Wade was not notified of the 2018 Data breach until several months after ABM gained knowledge of the same.

B. ***Stolen Information is Valuable to Hackers and Thieves***

24. It is well known, and the subject of many media reports, that PII, particularly medical information, is highly coveted and a frequent target of hackers. Businesses that utilize internet-based technologies are especially privy to data privacy issues and threats. Legitimate organizations and the criminal underground alike recognize the value of PII and they aggressively seek to pay for it.

25. PII can be sold in the cybercrime underground for lucrative retail values, especially where medical or financial information is involved. Such information can also be used to clone a credit card or forge an identity.

26. Notwithstanding their usage of internet-based technologies, their prior breach incident, and well-publicized litigation involving cybersecurity, ABM opted to maintain an insufficient and inadequate system to protect the PII of Plaintiffs and Class members.

C. ***Plaintiffs and Class Members Suffered Damages***

27. Plaintiffs and Class members now face years of constant surveillance of their financial and personal records. The Class is incurring and will continue to incur such damages;

fraudulent account charges and the resulting loss of use and access to their funds, regardless of whether such charges are ultimately reimbursed by the credit card companies; and other harms.

28. The Data Breaches were a direct and proximate result of ABM's failure to 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 the common law, including ABM's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

29. Plaintiffs' and Class members' PII is private and sensitive in nature and was inadequately protected by ABM. Compounding the problem, ABM did not obtain Plaintiffs' and Class members' consent to disclose their PII to unauthorized entities.

30. As a direct and proximate result of ABM's wrongful actions and inactions leading up to, surrounding, and following the subject Data Breaches, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the Data Breaches on their lives by, among other things, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

31. ABM's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. Theft of their PII and, on information and belief, actual identity theft;

b. The imminent and impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the Internet black market;

c. The untimely and inadequate notification of the Data Breaches to Plaintiffs

and the Class members;

d. The improper disclosure of their PII;

e. Loss of privacy;

f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breaches;

g. Ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market;

h. Loss in value of their employment with ABM in terms of the consideration they provided, *e.g.* employment services and their compliance with ABM's conditions of employment such as the provision of their PII, since ABM did not provide reasonable and adequate safeguards and security measures that would protect employees' and former employees' PII;

i. Deprivation of rights they possess under the various laws of California, Illinois, and New York; and

j. Other harms incurred by Plaintiffs and Class members due to the informational injuries incurred as a result of the deprivation of substantive data privacy rights conferred under the laws of California, Illinois, and New York, including rights conferred under statute and at common law.

CLASS ACTION ALLEGATIONS

32. Plaintiffs bring this action on their own behalf and on behalf of a nationwide class ("Class"), including a California Subclass ("California Subclass") and an Illinois Subclass ("Illinois Subclass"), of all other persons similarly situated, pursuant to California Civil Code § 1781, 735 ILCS § 5/2-801, and Fed. R. Civ. P. 23. The Class and Subclasses are defined as follows:

> **The Class**: All current and former ABM employees whose PII was disclosed in the 2017 Data Breach and/or the 2018 Data Breach (Counts I, VI, VII, VIII, IX, and X).
>
> **The California Subclass**: All current and former ABM employees or contractors residing in California whose PII was disclosed in the 2017 Data Breach and/or the 2018 Data Breach (Counts II, III, IV, V, XII).
>
> **The Illinois Subclass**: All current and former ABM employees or contractors residing in Illinois whose PII was disclosed in the 2017 Data Breach and/or the 2018 Data Breach (Count XI).

33. Plaintiffs do not know the exact number of members of the Class or Subclasses, since that information is within the exclusive control of Defendants. But the members of the Class and

Subclasses are believed to be in the tens of thousands. The Class and Subclasses are so numerous that joinder of all members is impracticable.

34. The Plaintiffs and the members of the Class and Subclasses share common interests, as they all have the same or similar claims arising from the same or similar wrongful actions and omissions of Defendants.

35. The claims and/or defenses of the Plaintiffs are typical of the claims and/or defenses of the Class and Subclasses and are all based upon the same legal theories. The Plaintiffs will fairly and adequately protect the interests of the Class and Subclasses. This class action is an appropriate method for the fair and efficient adjudication of the controversy. There are questions of law and/or fact common to the Class and Subclasses, which are substantially similar and predominate over the questions affecting the individual members. Common questions for the Class and Subclasses include, but are not limited to the following:

a. Whether Defendants adequately safeguarded Plaintiffs' and the Class members' PII;

b. Whether Plaintiffs and the Class members were notified of the 2017 Data Breach and/or the 2018 Data Breach within a reasonable period;

c. Whether Defendants willfully, recklessly, and/or negligently failed to maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and the Class members' PII;

d. Whether there was an unauthorized disclosure of the Class members' PII;

e. Whether implied or express contracts existed between Defendants and the Class members;

f. Whether Plaintiffs and the Class members sustained damages as a result of Defendants' failure to adequately safeguard their PII;

g. Whether Defendants' PII storage and protection protocols and procedures were reasonably compliant with industry standards;

h. Whether Defendants' cybersecurity prevention, detection, and notification protocols were reasonable under industry standards;

i. Whether Defendants misrepresented the safety and security of the Class members' PII maintained by Defendants;

j. Whether and/or when Defendants became aware of the unauthorized access to Plaintiffs' and the Class members' PII;

k. Whether Defendants' conduct violated California law;

l. Whether Defendants' conduct violated the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq*.; and

m. Whether Defendants' conduct violated New York General Business Law concerning Deceptive Acts and Practices, N.Y. Gen. Bus. Law § 349, *et seq.*

36. Absent a class action, most Class members would find the cost of litigating their claims to be prohibitively expensive and would have no effective remedy. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants and promotes consistency and efficiency of adjudication.

37. Plaintiffs will fairly and adequately represent and protect the interests of the other members of the Class and Subclasses they seek to represent. Plaintiffs have retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the other Class members and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Class or Subclasses.

38. Defendants have acted and failed to act on grounds generally applicable to the Plaintiffs and the other members of the Class and Subclasses, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class and Subclasses and making injunctive or corresponding declaratory relief appropriate for the Class and Subclasses as a whole.

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

39. Plaintiffs reallege and incorporate by reference the foregoing allegations as if fully set forth herein.

40. As a condition of employment, Defendants required Plaintiffs and the Class members

to provide their Private Identifiable Information.

41. Upon accepting and inputting Plaintiffs' and Class members' PII in their system, ABM undertook and owed a duty to Plaintiffs and Class members to exercise reasonable care to secure and safeguard that information from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties, and to utilize commercially reasonable methods to do so. This duty included, among other things, designing, maintaining, and testing ABM's security systems to ensure that Plaintiffs' and the Class members' PII was adequately secured and protected.

42. ABM also had a duty, or assumed a duty, to implement reasonable data privacy and cybersecurity protocols, including adequate prevention, detection, and notification procedures, in order to safeguard the PII of the Plaintiffs and the Class members and to prevent the unauthorized access to and disclosures of the same.

43. ABM also had a duty to timely disclose to Plaintiffs and Class members that their PII had been, or was reasonably believed to have been, compromised. Timely disclosure was appropriate so that, among other things, Plaintiffs and Class members could take appropriate measures to avoid theft of monies and to monitor their account information and credit reports for fraudulent activity.

44. Defendants breached these aforementioned duties in, without limitation, at least one or more of the following ways:

a. Failing to implement reasonable data privacy and cybersecurity measures to secure ABM's, and/or Plaintiffs' and Class members', email accounts, including failing to require adequate multifactor authentication and encryption;

b. Failing to implement a reasonable data privacy and cybersecurity protocol, including adequate procedures for preventing cybersecurity threats and/or detecting such threats in a timely manner;

c. Failing to notify Plaintiffs and Class members that their PII had been disclosed to nefarious hackers within a reasonable period of time, despite having specific knowledge of the same;

d. Failing to reasonably comply with applicable state and federal law concerning data privacy and cybersecurity protocol, including the substance of Defendants' unreasonably-delayed notification to Plaintiffs and Class members concerning the Data Breaches; and

e. Otherwise failing to act reasonably under the circumstances with regard to Defendants' conduct in preventing, detecting, and disclosing the Data Breaches.

45. ABM further breached their duty to discover and notify Plaintiffs and Class members by failing to discover the Data Breaches within a reasonable time and by failing to notify Plaintiffs and Class members of the Data Breaches until several months after ABM gained knowledge of the respective Data Breaches. To date, ABM have not provided sufficient information to Plaintiffs and Class members regarding the extent and scope of the Data Breaches and continue to violate their legal disclosure obligations to Plaintiffs and the Class.

46. ABM also breached their duty to Plaintiffs and Class members to adequately protect and safeguard their PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured networks. ABM's conduct permitted third parties to gather Plaintiffs' and Class members' PII, misuse it, and intentionally disclose and sell it to others without consent.

47. Defendants knew, or should have known, that their data privacy and cybersecurity protocol failed to reasonably protect Plaintiffs' and the Class members' PII.

48. Through their failure to timely discover and provide clear notification of the Data Breaches to consumers, ABM prevented Plaintiffs and Class members from taking meaningful, proactive steps to secure their data.

49. Upon information and belief, ABM improperly and inadequately safeguarded the PII of Plaintiffs and Class members in deviation from standard industry rules, regulations, and practices at the time of the Data Breaches.

50. ABM's failure to take proper security measures to protect Plaintiffs' and Class members' sensitive PII created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access, theft, and sale of Plaintiffs' and Class members' PII.

51. ABM's conduct was grossly negligent and departed from all reasonable standards of care, including but not limited to: failing to adequately protect the PII; failing to conduct adequate regular security audits; and failing to provide adequate and appropriate supervision of persons

having access to Plaintiffs' and Class members' PII.

52. Defendants' failure to implement a cybersecurity and data privacy governance program and to properly train their current and former employees to detect, avoid, and report cyberthreats such as phishing attempts resulted in the Plaintiffs and the Class members being unequipped to avoid the Data Breaches.

53. Defendants' lax, non-compliant, inadequate, and/or nonexistent cybersecurity governance program not only allowed unauthorized third parties to infiltrate their corporate networks, but also enabled such hackers to go undetected for an extended period. Had Defendants employed an adequate cybersecurity protocol, the unauthorized third parties would not have been able to transmit malware to ABM employees and extract data from their firewall.

54. As a direct result of Defendants' negligent acts and omissions, Plaintiffs and the Class members suffered injury and damages, including the loss or substantial impairment of their legally protected interest in the confidentiality and privacy of their PII, the loss or substantial impairment of the benefit of their bargain in accepting employment with Defendants, and pecuniary injury in the form of time and expense to mitigate the disclosure of their data to nefarious third parties.

COUNT II

Violation of California's Unfair Competition Law Cal. Bus. & Prof. Code § 17200 Unlawful Business Practices

(On Behalf of Plaintiff Davila and the California Subclass)

55. Plaintiff Davila realleges and incorporates by reference the foregoing allegations as if fully set forth herein.

56. ABM have violated Cal. Bus. and Prof. Code §17200 *et seq*. by engaging in unlawful, unfair or fraudulent business acts and practices, as defined in Cal. Bus. Prof. Code §17200. ABM engaged in unlawful acts and practices with respect to their services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and Class members' PII with knowledge that the information would not be adequately protected; and by gathering Plaintiff's and the California Subclass members' PII in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which

required ABM to take reasonable methods of safeguarding the PII of Plaintiff and the California Subclass members.

57. In addition, ABM engaged in unlawful acts and practices with respect to their services by failing to discover and then disclose the Data Breaches to Plaintiff and the California Subclass members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82. To date, ABM have still not provided sufficient information to Plaintiff and the California Subclass members.

58. As a direct and proximate result of ABM's unlawful acts and practices, Plaintiff and the California Subclass members were injured and lost money or property, including but not limited to the loss or substantial impairment of their legally protected interest in the confidentiality and privacy of their PII, and additional losses described above.

59. ABM knew or should have known that their system had been breached, that their data security practices were inadequate to safeguard California Subclass members' PII, and that the risk of a data breach or theft was highly likely. ABM's actions in engaging in the above-named unlawful practices and acts were at least negligent, if not reckless and/or willful with respect to the rights of the California Subclass members.

60. Plaintiff and the California Subclass members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiff and California Subclass members of money or property that ABM may have acquired by means of their unlawful and unfair business practices, restitutionary disgorgement of all profits accruing to ABM because of their unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT III

Violation of California's Unfair Competition Law Cal. Bus. & Prof. Code §17200 Unfair Business Practices

(On Behalf of Plaintiff Davila and the California Subclass)

61. Plaintiff Davila realleges and incorporates by reference the foregoing allegations as if fully set forth herein.

62. ABM engaged in unfair acts and practices by soliciting and collecting Plaintiff's and

the California Subclass members' PII with knowledge that the information would not be adequately protected and that Plaintiff's and the California Subclass members' PII would be processed in an unsecure electronic environment. ABM also engaged in unfair acts and practices with respect to the provision of their services by failing to enact adequate privacy and security measures and protect California Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, and by failing to timely discover and give notice of the Data Breaches.

63. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and the California Subclass members. They were likely to deceive the public into believing their PII was secure, when it was not. The harm these practices caused to Plaintiff and the California Subclass members outweighed their utility, if any.

64. As a direct and proximate result of ABM's unfair acts and practices, Plaintiff and the California Subclass members were injured and lost money or property, including but not limited to the loss or substantial impairment of their legally-protected interest in the confidentiality and privacy of their PII, and additional losses described above.

65. ABM knew or should have known that their systems and data security practices were inadequate to safeguard California Subclass members' PII and that the risk of a data breach or theft was highly likely. ABM's actions in engaging in the above-named unlawful practices and acts were at least negligent, if not reckless and/or willful.

66. The members of the California Subclass seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including but not limited to, restitution to Plaintiff and the California Subclass members of money or property that ABM may have acquired by means of their unfair business practices, restitutionary disgorgement of all profits accruing to ABM because of their unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. §1021.5), and injunctive or other equitable relief.

COUNT IV
Violation of California's Unfair Competition Law Cal. Bus. & Prof. Code §17200
Fraudulent/Deceptive Business Practices
(On Behalf of Plaintiff Davila and the California Subclass)

67. Plaintiff Davila realleges and incorporates by reference the foregoing allegations as if fully set forth herein.

68. ABM engaged in fraudulent and deceptive acts and practices by omitting, suppressing, and concealing the material fact of the inadequacy of their privacy and security protections for California Subclass members' PII. At the time that California Subclass members were using ABM's system, ABM failed to disclose to the Subclass members that their data security systems failed to meet legal and industry standards for the protection of their PII. Plaintiff and the California Subclass members would not have entrusted ABM with their private information if they had known about ABM's substandard data security practices. These representations were likely to deceive members of the public, including Plaintiff and the California Subclass members, into believing their PII was secure, when it was not, and that ABM were complying with relevant law and industry standards, when they were not.

69. As a direct and proximate result of ABM's deceptive practices and acts, Plaintiff and the California Subclass members were injured and lost money or property, including but not limited to the loss of their legally protected interest in the confidentiality and privacy of PII, and additional losses described above.

70. ABM knew or should have known that their system and data security practices were inadequate to safeguard California Subclass members' PII and that the risk of a data breach or theft was highly likely. ABM's actions in engaging in the above-named unlawful practices and acts were at least negligent, if not reckless and/or willful.

71. The members of the California Subclass seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiffs and the California Subclass members of money or property that ABM may have acquired by means of their fraudulent and deceptive business practices, restitutionary disgorgement of all profits accruing to ABM because of their fraudulent and deceptive business practices, declaratory relief, attorney's fees and costs

(pursuant to Cal. Code Civ. Proc. §1021.5), and injunctive or other equitable relief.

COUNT V
Constitutional Invasion of Privacy
(On Behalf of Plaintiff Davila and the California Subclass)

72. Plaintiff Davila realleges and incorporates by reference the foregoing allegations as if fully set forth herein.

73. Article 1, Section 1, of the California Constitution provides that "[a]ll people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

74. Plaintiff and the California Subclass members had a legally protected privacy interest in their PII provided to ABM.

75. Plaintiff and the California Subclass members had a reasonable expectation of privacy as to the PII they provided to ABM.

76. ABM's actions and inactions amounted to a serious invasion of the protected privacy interests of Plaintiff and the California Subclass members.

77. ABM's invasion of Plaintiff's and the California Subclass members' reasonable expectation of privacy caused Plaintiff and the California Subclass members to suffer damages.

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

78. Plaintiffs reallege and incorporate by reference the foregoing allegations as if fully set forth herein.

79. ABM had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class members' PII, pursuant to state laws in California, Illinois, and New York:

a. California Civil Code § 1798.81.5;

b. California Civil Code § 56, *et seq.*;

c. Illinois Consumer Fraud and Deceptive Business Practices Act 815 ILCS

505/1, *et seq.*;

d. Illinois Personal Information Protection Act 815 530/1, *et seq.*; and

e. New York General Business Law § 349, *et seq*.

80. ABM breached their duties to the Class members as established under the laws stated above by failing to provide fair, reasonable, and/or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' PII, and by failing to implement and conduct a reasonable and adequate breach notification protocol in a timely manner.

81. ABM's failure to comply with applicable laws constitutes negligence *per se*.

82. But for ABM's wrongful and negligent breach of their duties owed to Plaintiffs and Class members, Plaintiffs and the Class members would not have been injured in the manner described herein.

83. The injuries and harms suffered by Plaintiffs and the Class members were the reasonably foreseeable result of ABM's breach of their duties. ABM knew or should have known that they were failing to meet their duties, and that ABM's breach would cause Plaintiffs and the Class members to experience the foreseeable harms associated with the exposure of their PII.

84. As a direct and proximate result of ABM's negligent conduct, Plaintiffs and the Class members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT VII
Violation of State Data Breach Acts
(On Behalf of Plaintiff Davila and the California Subclass)

85. Plaintiff Davila realleges and incorporates by reference the foregoing allegations as if fully set forth herein.

86. ABM own, license, and/or maintain computerized data that includes Plaintiff's and the California Subclass members' PII.

87. ABM were required, but failed, to take all reasonable steps to dispose, or arrange for the disposal, of records within their custody or control containing PII when the records were no longer needed, by shredding, erasing, or otherwise modifying the identifying information in those records to make it unreadable or undecipherable through any means.

88. ABM's conduct, as alleged above, violated the data breach statutes of California, including California, Cal. Civ. Code §§ 1798.80 *et seq*.

89. ABM were required, but failed, to implement reasonable cybersecurity practices appropriate to the nature and scope of the information compromised in the Data Breaches.

90. The Data Breaches constituted a "breach of the security system" within the meaning of section 1798.82(g) of the California Civil Code.

91. The information compromised in the Data Breaches constituted "personal information" within the meaning of section 1798.80(e) of the California Civil Code.

92. Like other state Data Breach Acts, California Civil Code § 1798.80(e) requires disclosure of data breaches "in the most expedient time possible and without unreasonable delay."

93. ABM violated Cal. Civ. Code § 1798.80(e) by unreasonably delaying disclosure of the Data Breaches to Plaintiff and other California Subclass members, whose PII was, or was reasonably believed to have been, acquired by an unauthorized person.

94. Upon information and belief, no law enforcement agency instructed ABM that notification to Plaintiff and the California Subclass members would impede a criminal investigation; thus, such notification was required.

95. ABM 's violation of state Data Breach Acts, including Cal. Civ. Code § 1798.80, *et seq.*, directly and proximately caused Plaintiff and the California Subclass members to incur economic damages, including expenses associated with monitoring their personal and financial information to prevent further fraud.

96. Plaintiff, individually and on behalf of the California Subclass, seeks all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to: (a) actual damages suffered by California Subclass members as alleged above; (b) statutory damages for ABM's willful, intentional, and/or reckless violation of Cal. Civ. Code § 1798.83; (c) equitable relief; and (d) reasonable attorneys' fees and costs under Cal. Civ. Code §1798.84(g).

97. Because ABM were guilty of oppression, fraud or malice, in that they acted with a willful and conscious disregard of Plaintiff's and the California Subclass members' rights, Plaintiff also seek punitive damages, individually and on behalf of the California Subclass.

COUNT VIII

Violation of N.Y. Gen. Bus. Law § 349, *et seq.*

(On Behalf of Plaintiffs and the Class and Subclasses)

98. Plaintiffs reallege and incorporate by reference the foregoing allegations as if fully set forth herein.

99. Defendants are headquartered in New York.

100. Defendants engaged in deceptive, unfair and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, *et seq*., including but not limited to the following acts and omissions:

a. Misrepresenting the adequacy of their data privacy and cybersecurity practices and procedures to safeguard the Class Members' PII;

b. Requiring the provision of PII by the Class members as a condition of employment despite the inadequacy of their cybersecurity protocol;

c. Failing to take reasonable measures to mitigate the disclosure of Class members' PII, including failing to notify the Class members of such unauthorized disclosures of their PII until more than seven months after they learned of the Data Breaches and failing to promptly identify the source of the Data Breaches;

d. Concealing the material fact of the inadequacy of their privacy and security protections for the Class members' PII;

e. Otherwise engaging in a course of conduct that is contrary to accepted data privacy, cybersecurity and personnel management standards; and

f. Otherwise engaging in deceptive, unfair and unlawful trade acts or practices by failing to maintain the sensitive PII of the Class members in violation of the duties and public policies reflected in applicable state and federal laws.

101. As a direct result of Defendants' deceptive, unfair, and unlawful trade practices, Plaintiffs and the Class members suffered injury and damages, including the loss of their legally protected interest in the confidentiality and privacy of their PII, the loss of the benefit of their bargain in accepting employment with Defendants, pecuniary injury in the form of time and expense to mitigate the disclosure of their PII to nefarious third parties.

102. Had Defendants provided timely and accurate notice of the Data Breaches, Plaintiffs and the Class members would have been able to mitigate or attempt to mitigate the damages and

harm resulting in Defendants' failure to prevent the Data Breaches and their unreasonable delay in providing notice to the Class members by, for example, the purchase of credit monitoring services, placement of alerts on their financial accounts, and other identify theft measures.

103. Defendants knew, or should have known, that their data privacy and cybersecurity practices were inadequate to safeguard the Plaintiffs' and the Class members' PII and that the risk of a data breach or theft was highly likely.

104. Defendants' conduct was knowing and willful and/or wanton and reckless, and at the very least was highly negligent, with respect to the rights of Plaintiffs and the Class members.

COUNT IX
Breach of Contract
(On Behalf of Plaintiffs and the Class and Subclasses)

105. Plaintiffs reallege and incorporate by reference the foregoing allegations as if fully set forth herein.

106. Plaintiffs and Class members are parties to express agreements with Defendants whereby Plaintiffs and the Class members provide labor, their PII, and other employment-related services to Defendants in exchange for compensation and other material, employment-related benefits, including the provision of reasonable safeguards to prevent the unauthorized disclosure of Plaintiffs' and Class members' PII. Plaintiffs and the Class members fully performed their obligations under their employment agreements with Defendants.

107. Defendants' failure to implement an adequate and reasonable data privacy and cybersecurity protocol which included adequate prevention, detection, and notification procedures constitutes a breach of contract.

108. Plaintiffs and the Class members would not have provided and entrusted their PII to Defendants as a condition of employment with Defendants, or would have sought additional compensation, in the absence of an agreement with Defendants to reasonably safeguard their PII and to reasonably notify them of unauthorized disclosures.

109. Defendants breached the contracts they made with Plaintiffs and the Class members by failing to safeguard and protect their PII, and by failing to notify them in a timely and accurate manner that that their PII was compromised in the Data Breaches.

110. The damages expressed herein as sustained by Plaintiffs and the Class members were the direct and proximate result of Defendants' breaches of contract.

COUNT X
Breach of Implied Contract (in the alternative to Count IX)
(On Behalf of Plaintiffs and the Class and Subclasses)

111. Plaintiffs reallege and incorporate by reference the foregoing allegations as if fully set forth herein.

112. Plaintiffs and the Class members were required to provide Defendants their PII as a condition of employment. In the alternative to Count IX, and to the extent that it is found that Defendants did not have an express contract with Plaintiffs and the Class members, Defendants entered into contracts-implied-in-fact with Plaintiffs and the Class members whereby, by virtue of the requirement to provide their PII, Defendants were obligated to take reasonable steps to secure and safeguard the Class members' PII, and Defendants were obligated to take reasonable steps following the Data Breaches to disclose the material details regarding the same.

113. Defendants' failure to implement an adequate and reasonable data privacy and cybersecurity protocol which included adequate prevention, detection, and notification procedures constitutes a breach of an implied contract between Defendants and the Class members.

114. Plaintiffs and the Class members would not have provided and entrusted their PII to Defendants to obtain employment with Defendants, or would have sought additional compensation, in the absence of an agreement with Defendants to reasonably safeguard their PII and to reasonably notify them of unauthorized disclosures

115. Plaintiffs and the Class members fully performed their obligations under their implied contracts with Defendants.

116. Defendants breached the implied contracts they made with Plaintiffs and the Class members by failing to safeguard and protect their PII, and by failing to notify them in a timely and accurate manner that that their PII was compromised in the Data Breaches.

117. The damages expressed herein as sustained by Plaintiffs and the Class members were the direct and proximate result of Defendants' breaches of contract.

COUNT XI
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*
(On Behalf of Plaintiff Wade and the Illinois Subclass)

118. Plaintiff Wade realleges and incorporates by reference the foregoing allegations as if fully set forth herein.

119. Pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq.* ("IPIPA"), Defendants were required to implement and maintain reasonable security measures to protect Plaintiff's and the Illinois Subclass members' PII and to notify them regarding any unauthorized disclosure in the most expedient time possible and without reasonable delay.

120. Defendants' unlawful conduct alleged herein in failing to safeguard their employees' PII and subsequent failure to notify their employees that such PII had been compromised as required constitute violations of the IPIPA.

121. Pursuant to Section 530/20 of the Illinois Consumer Fraud and Deceptive Business Practices Action, 815 ILCS 505/1, *et seq.*, a violation of IPIPA is deemed an unlawful practice and violation of the Illinois Consumer Fraud and Deceptive Business Practices Act. *See* 815 ILCS 505/20.

122. Plaintiff and the Illinois Subclass members have suffered injury in fact and actual damages, as alleged herein, as a result of Defendants' unlawful conduct and violations of the Illinois Consumer Fraud and Deceptive Business Practices Act.

COUNT XII
Violation of the California Confidentiality of Medical Information Act (Cal. Civ. Code § 56, *et seq.)*
(On Behalf of Plaintiff Davila and the California Subclass).

123. Plaintiff Davila realleges and incorporates by reference the foregoing allegations as if fully set forth herein.

124. Cal. Civ. Code § 56, *et seq*. requires employers that receive medical information from employees to design, implement, and maintain procedures to ensure the confidentiality and protection from unauthorized use and disclosure of such information. Cal. Civ. Code § 56 also prohibits employers from the disclosure of such information without first obtaining written consent.

125. ABM were in the possession of, and retained, medical information belonging to and regarding their current and former employees.

126. Cal. Civ. Code § 56, *et seq.*, imposed a legal duty on ABM to protect the confidential and highly sensitive medical information of Plaintiffs and the California Subclass.

127. ABM failed to develop, implement, and maintain data security and retention policies that would have prevented the access to Plaintiff's and the California Subclass members' PII, including medical information, without prior written authorization.

128. As such, ABM breached their legal duties imposed by Cal. Civ. Code § 56, *et seq.*

129. Cal. Civ. Code § 56.36 entitles Plaintiff and the California Subclass members who had medical information compromised during the Data Breaches to nominal damages of $1,000.00 per California Subclass member, in addition to actual damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Evelia Davila and Larry Wade, individually and on behalf of all Class and Subclass members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendants ABM as follows:

A. For an Order certifying the Class, California Subclass, and Illinois Subclass as defined herein and appointing Plaintiffs as Class Representatives and their undersigned attorneys as Class Counsel to represent the Class and Subclasses;

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

C. For equitable relief compelling ABM to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity to Class members the type of PII compromised;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully

retained as a result of ABM 's wrongful conduct;

E. For an award of actual damages, treble damages, statutory damages, compensatory damages, nominal damages, and punitive damages in an amount to be determined at trial;

F. For an award of attorneys' fees and costs of suit, as allowable by law; and

G. For such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and all others similarly situated, hereby demand a jury trial for all claims so triable.

DATED: April 26, 2019

By: /s/ Jad Sheikali
One of the Attorneys for Plaintiffs

Jad Sheikali (*pro hac vice*)
jsheikali@mcgpc.com
David L. Gerbie (*pro hac vice*)
dgerbie@mcgpc.com
MCGUIRE LAW, P.C.
55 West Wacker Drive, 9th Floor
Chicago, Illinois 60601
Telephone: (312) 893-7002
Facsimile: (312) 275-7895

Thomas V. Girardi, (SBN: 36603)
tgirardi@girardikeese.com
Keith D. Griffin, (SBN: 204388)
kgriffin@girardikeese.com
GIRARDI | KEESE
1126 Wilshire Boulevard
Los Angeles, California 90017
Telephone: (213) 977-0211
Facsimile: (213) 481-1554

Ebby S. Bakhtiar (SBN: 215032)
esb@livingstonbakhtiar.com
LIVINGSTON • BAKHTIAR.
3435 Wilshire Boulevard, Suite 1669
Los Angeles, CA 90010
Telephone: (213) 632-1550