David S. Casey, Jr., SBN 060768
dcasey@cglaw.com
Gayle M. Blatt, SBN 122048
gmb@cglaw.com
Jeremy Robinson, SBN 188325
jrobinson@cglaw.com
P. Camille Guerra, SBN 326546
camille@cglaw.com
James M. Davis, SBN 301636
jdavis@cglaw.com
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

NOREEN PFEIFFER, JOSE CONTRERAS and **SUSAN WRIGHT**, on behalf of themselves and all other persons similarly situated,

Plaintiffs,

v.

RADNET, INC., a Delaware corporation,

Defendant.

CASE NO. 2:20-cv-9553

CLASS ACTION COMPLAINT

Demand for Jury Trial

Plaintiffs Noreen Pfeiffer, Jose Contreras and Susan Wright, individually, and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to them and on information and belief as to all other matters, by and through undersigned counsel, hereby bring this Class Action Complaint against Defendant RadNet, Inc., and allege as follows:

INTRODUCTION

1. Obtaining a job requires turning over to employers valuable personal identifying information ("PII"), including social security numbers, driver's license numbers, birth dates and addresses. If stolen, identity thieves can use this highly sensitive information to fraudulently open new accounts, access existing accounts, perpetrate identity fraud or impersonate victims in myriad schemes, all of which can cause grievous financial harm, negatively impact the victim's credit scores for years, and cause victims to spend countless hours mitigating the impact.

2. Despite the dire warnings about the severe impact of data breaches on Americans of all economic strata, companies still fail to put adequate security measures in place to protect their customers' and employees' data.

3. Defendant RadNet, Inc. ("RadNet"), a provider of outpatient imaging, is among those companies that failed to meet its obligation to protect the sensitive personal identifying information entrusted to it by their current and former employees.

4. As a corporation doing business in California, RadNet is legally required to protect the PII it gathers from unauthorized access and exfiltration.

5. Defendant RadNet collected its employees' sensitive PII. And in acquiring various imaging centers, Defendant collected the PII of employees of those businesses. In either case, Defendant had an obligation to secure that PII by implementing reasonable and appropriate data security.

6. On or about July 18, 2020, an unknown third party gained unauthorized access to a RadNet server that was used to store certain employee data, and copied

files to an external server. The unlawfully access information included employee names, social security numbers, driver's license numbers, and additional data such as dates of birth, addresses, and passport numbers.

7. As a result of RadNet's failure to provide adequate data security, Plaintiffs' and the Class members' PII has been exposed to those who should not have access to it. Plaintiffs and the Class are now at much higher risk of identity theft and for cybercrimes of all kinds.

THE PARTIES

8. Defendant Radnet, Inc., is a Delaware corporation with its principal place of business in Los Angeles, California.

9. Plaintiff Noreen Pfeiffer is a resident of Cockeysville, Maryland. She was employed by Medical Imaging of Baltimore from June 1988 until January 2012. As a part of her employment, she provided that entity with her PII.

10. Medical Imaging of Baltimore was acquired by RadNet before the data breach at issue herein. In or about January 2012, following RadNet's acquisition of Medical Imaging of Baltimore, Pfeiffer became an employee of RadNet and began to receive compensation from RadNet. As part of the acquisition of Medical Imaging of Baltimore, RadNet acquired and stored the PII that Plaintiff Pfieffer had provided to that company as a part of her employment.

11. Pfeiffer reasonably believed RadNet would keep her PII secure. Had RadNet disclosed to Pfeiffer that her PII would not be kept secure and would be left easily accessible to hackers and third parties, she would have taken additional precautions relating to her PII.

12. Plaintiff Susan Wright is a resident of Edgewood, Maryland. She was employed by Advanced Imaging Partners, Inc. from May 1988 to June 2020. As a part of her employment, she provided that entity with her PII.

13. Advanced Imaging Partners, Inc. was acquired by RadNet before the data breach at issue herein. RadNet is the controlling company of Advanced Imaging

Partners, Inc. As part of the acquisition of Advanced Imaging Partners, Inc., RadNet acquired and stored the PII that Plaintiff Wright had provided to that company as a part of her employment.

14. Wright reasonably believed RadNet would keep her PII secure. Had RadNet disclosed to Wright that her PII would not be kept secure and would be kept easily accessible to hackers and third parties, she would have taken additional precautions relating to her PII.

15. Plaintiff Jose Contreras is a resident of Pacoima, California. He was employed by RadNet San Fernando Valley Northridge Diagnostic Imaging Center from approximately 2006 to 2016.

16. Contreras reasonably believed RadNet would keep his PII secure. Had RadNet disclosed to Contreras that his PII would not be kept secure and would be kept easily accessible to hackers and third parties, he would have taken additional precautions relating to his PII.

JURISDICTION AND VENUE

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

18. This Court has personal jurisdiction over Defendant because it maintains its principal place of business in this District, is registered to conduct business in California, and has sufficient minimum contacts with California.

19. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant resides in this District and, on information and belief, a substantial part of the events or omissions giving rise to Plaintiffs' and Class members' claims occurred in this District.

20. Application of California law to this dispute is proper because Defendant's headquarters are in California, the decisions or actions that gave rise to

the underlying facts at issue in this Complaint were presumably made or taken in California, and the action and/or inaction at issue emanated from California.

FACTUAL ALLEGATIONS

A. RadNet Collects and Stores Thousands of Employees' and Former Employees' PII and Fails to Provide Adequate Data Security

21. RadNet is a publicly traded company with a market capitalization approaching one billion dollars. It is a major player in its industry. In addition to a full range of medical imaging solutions, it also operates an IT division which delivers integrated, web-based, cloud solutions for medical imaging workflow.[1] RadNet also provides a "sophisticated portfolio of insurance solutions to physicians" and operates RadNet TV delivering "targeted, dynamic programming for patients, family members, friends, and guests."[2]

22. On July 18, 2020, an unknown third party gained access to a RadNet server that was used to store employee data and copied files to an external server.

23. Employee names, social security numbers, driver's license numbers, as well as dates of birth, addresses, and passport numbers were among the PII that may have been accessed by the unknown third party.

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

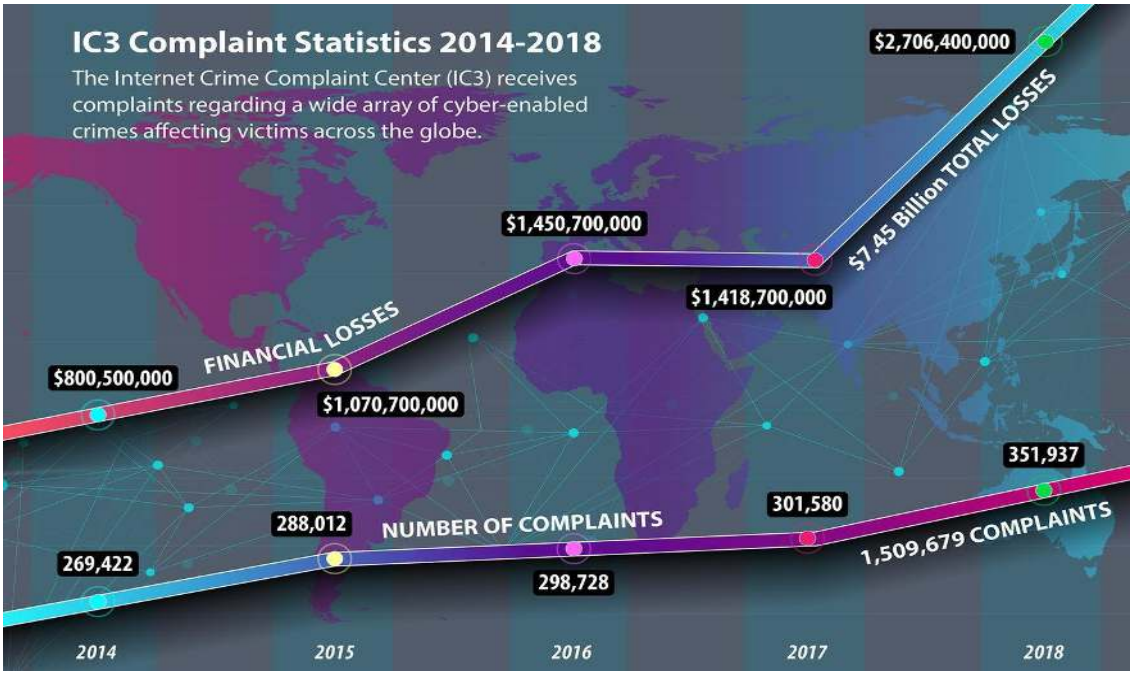
25. On or about September 28, 2020, Plaintiffs Pfeiffer, Jose Contreras and Wright received a letter titled "Notice of Data Breach," dated September 21, 2020, from RadNet. The letter stated that their PII, including those mentioned above, may have been compromised.

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

---

[1] https://www.radnet.com/
[2] *Id.*

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



28. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

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

30. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends and colleagues of the original victim.

31. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

32. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Here, Defendant did not rapidly report to Plaintiffs and Class Members that their PII had been stolen. Instead, it took Defendant almost two months to notify them.

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

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

35. For example, The United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[3] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[4]

B. RadNet Failed to Comply with Federal Trade Commission Requirements

36. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has

---

[3] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), available at http://www.gao.gov/assets/270/262899.pdf (last visited October 6, 2020).

[4] *Id.*

issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[5]

37. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[6] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[7]

38. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[8]

39. Highlighting the importance of protecting against data breaches, the FTC has brought enforcement actions against businesses for failing to adequately and

---

[5] *See* Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited October 6, 2020).

[6] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last October 6, 2020).

[7] *Id.*

[8] Federal Trade Commission, *Start With Security*, *supra* note 6.

reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[9]

40. By allowing an unknown third party to access a RadNet server and copy employee PII to an unknown server, RadNet failed to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee data. RadNet's data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

CLASS ACTION ALLEGATIONS

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

a. The Nationwide Class:

All persons residing in the United States who are employees or former employees of RadNet or any affiliate, parent, or subsidiary of RadNet who had their PII compromised as a result of the Data Breach that occurred on or about July 18, 2020.

b. The California Subclass:

All persons residing in the State of California who are employees or former employees of RadNet or any affiliate, parent, or subsidiary of RadNet who had their PII compromised as a result of the Data Breach that occurred on or about July 18, 2020.

42. Collectively, the Nationwide Class and the California Subclass will be referred to as "the Class" unless there is a need to differentiate them.

---

[9] Federal Trade Commission, *Privacy and Security Enforcement Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited October 6, 2020).

43. Excluded from the proposed Class are any officer or director of RadNet; any officer or director of any affiliate, parent, or subsidiary of RadNet; anyone employed by counsel in this action; and any judge to whom this case is assigned, his or her spouse, and members of the judge's staff.

44. **Numerosity.** Members of the proposed Class are large in number and are too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendant's own records.

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

a. Whether Defendant engaged in the wrongful conduct alleged herein;
b. Whether Defendant's inadequate data security measures were a cause of the data security breach;
c. Whether Defendant owed a legal duty to Plaintiffs and the other Class members to exercise due care in collecting, storing, and safeguarding their PII;
d. Whether Defendant negligently or recklessly breached legal duties owed to Plaintiffs and the other class members to exercise due care in collecting, storing, and safeguarding their PII;
e. Whether Plaintiffs and the Class are at an increased risk for identity theft because of the data security breach;
f. Whether Defendant's conduct violated Cal. Bus. & Prof. Code § 17200 *et seq.*;
g. Whether Defendant violated section 1798.150 of the California Consumer Privacy Act by failing to prevent Plaintiffs' and Class members' PII from unauthorized access and exfiltration, theft, or disclosure, as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information;
h. Whether Plaintiffs and the other class members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

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

46. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the other Class members. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

47. **Typicality:** The claims of Plaintiffs Noreen Pfeiffer and Susan Wright are typical of the claims of the members of the National Class. The claims of Plaintiff Jose Contreras are typical of the claims of the members of the California Subclass. All Class members were subject to the Data Breach and had their PII accessed by and/or disclosed to unauthorized third parties.

48. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class members they seek to represent; they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

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

presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

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

50. Plaintiffs incorporate by reference all previous allegations as though fully set forth herein.

51. Defendant violated and continues to violate California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq*., which prohibits unlawful, unfair, and/or fraudulent business acts or practices.

52. Defendant's conduct, as alleged above, is unlawful because it violates state data security laws, including the California Consumer Protection Act, as well as Section 5 of the Federal Trade Commission Act, which prohibits "unfair … practices in or affecting commerce."

53. Defendant's failure to safeguard Plaintiffs' and Class members' PII is an unfair practice under the UCL because the gravity of harm to Plaintiffs and Class members outweighs the utility of Defendant's conduct. This conduct includes Defendant's failure to adequately ensure the privacy, confidentiality, and security of employee data entrusted to it and Defendant's failure to have adequate data security measures in place. Current and former employees of Defendant were harmed because they were obligated to provide sensitive and confidential information in order to obtain or continue employment, and Defendant failed to provide such security.

54. Indeed, the PII of Plaintiffs and Class members, including their names, Social Security numbers, driver's license numbers, birth dates, addresses, and passport numbers, were made accessible by Defendant to unauthorized third parties, subjecting Plaintiffs and the Class members to an impending risk of identity theft.

55. As a direct result of Defendant's violations of the UCL, as set out above, Plaintiffs and the Class members suffered injury in fact and lost money or property by not being adequately compensated for the heightened risks they were taking by providing their PII.

56. As a direct result of Defendant's violations of the UCL, Plaintiffs and the Class members are entitled to restitution and other equitable relief.

SECOND CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

57. Plaintiffs incorporate by reference all previous allegations as though fully set forth herein.

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

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

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

61. Plaintiffs and members of the Class entrusted Defendant with their PII with the understanding that Defendant would safeguard their information, and Defendant was in a position to protect against the harm suffered by Plaintiffs and

members of the Class as a result of the Data Breach.

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

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

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

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

66. Defendant had a special relationship with Plaintiffs and Class members by virtue of being Plaintiffs' and Class members' current or former employees. Plaintiffs and Class members reasonably believed that Defendant would take adequate security precautions to protect their PII.

67. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiffs' and Class members' PII.

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

69. In engaging in the negligent acts and omissions as alleged herein, which permitted an unknown third party to access a RadNet server containing current and

former employee PII, Defendant violated Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce." This prohibition includes failing to have adequate data security measures and failing to protect their current and former employees' PII.

70. Plaintiffs and the Class members are among the class of persons Section 5 of the FTC Act was designed to protect, and the injuries suffered by Plaintiffs and the Class members is the type of injury Section 5 of the FTC Act was intended to prevent. As a result, Defendant is negligent per se.

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

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

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

73. Plaintiffs incorporate by reference all previous allegations as though fully set forth herein.

74. Defendant offered employment to Plaintiffs and Class members, either directly or through acquiring the businesses for which Plaintiffs and Class members worked. Defendant either required Plaintiffs and Class members to provide their PII or acquired their PII, including names, addresses, dates of birth, Social Security numbers, driver's license numbers, passport numbers and other personal information, from their former employers which Defendant acquired.

75. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiffs and Class members in its possession was only used to provide the agreed-upon compensation and other employment benefits from Defendant.

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

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

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

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

80. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiffs and Class members, Plaintiffs and the Class members

suffered damages as described in detail above.

FOURTH CAUSE OF ACTION
Violation of the California Consumer Privacy Act, Cal. Civ. Code § 1798.150 (On Behalf of Plaintiff Contreras and the California Subclass)

81. Plaintiff Contreras incorporates by reference all previous allegations as though fully set forth herein.

82. Defendant collects consumers' personal information as defined in Cal. Civ. Code § 1798.140. As a result, Defendant has a duty to implement and maintain reasonable security procedures and practices to protect this personal information. As alleged herein, Defendant failed to do so.

83. Defendant violated § 1798.150 of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiff Contreras' and California Subclass members' nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure. These failures were the result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

84. As a direct and proximate result of Defendant's conduct, Plaintiff Contreras's and the California Subclass members' personal information, including names, social security numbers, driver's license numbers, and additional data such as dates of birth, addresses, and passport numbers, was subjected to unauthorized access, exfiltration, and theft. On information and belief, Plaintiff Conreras and the California Subclass allege this PII was not encrypted or redacted in the format accessed during the Data Breach.

85. Plaintiff Contreras and the California Subclass members seek injunctive or other equitable relief to ensure Defendant hereafter adequately safeguards customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold customers' PII, including that of Plaintiff Contreras and the California Subclass. These individuals

have an interest in ensuring that their PII is reasonably protected.

86. On October 17, 2020, Plaintiffs' Counsel sent a notice letter to Defendant's registered service agent via FedEx Priority. Assuming Defendant cannot cure the Data Breach within 30 days, and Plaintiffs believe any such cure is not possible under these facts and circumstances, Plaintiffs intend to promptly amend this complaint to seek actual damages and statutory damages of no less than $100 and up to $750 per customer record subject to the Data Breach on behalf of the California Subclass as authorized by the CCPA.

PRAYER FOR RELIEF

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

a. Certifying the proposed Class as requested herein;
b. Appointing Plaintiffs as Class Representatives and undersigned counsel as Class Counsel;
c. Finding that Defendant engaged in the unlawful conduct as alleged herein;
d. Enjoining Defendant's conduct and requiring Defendant to implement proper data security policies and practices;
e. Awarding Plaintiffs and Class members damages;
f. Awarding Plaintiffs and Class members pre-judgment and post-judgment interest on all amounts awarded;
g. Awarding Plaintiffs and the Class members reasonable attorneys' fees, costs, and expenses; and

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

DEMAND FOR JURY TRIAL

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

Dated: October 17, 2020

/s/ Gayle M. Blatt
GAYLE M. BLATT

CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP

Attorneys for Plaintiffs and the putative Class