

**IN THE CIRCUIT COURT OF THE NINTH JUDICIAL CIRCUIT
IN AND FOR ORANGE COUNTY, FLORIDA**

DEBRA MARINO, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

MULLINAX FORD OF CENTRAL
FLORIDA, INC.,

Defendant.

Case No.: 2026-CA-004289-O

JURY DEMAND

AMENDED CLASS ACTION COMPLAINT

INTRODUCTION

1. Representative Plaintiffs Debra Marino, Myra Reames-Clevenger, and Shirley Rohr (“Representative Plaintiffs”) bring this amended class action against Defendant Mullinax Ford of Central Florida, Inc. (“Defendant”) for its failure to properly secure and safeguard Representative Plaintiffs’ and/or Class Members’ personally identifiable information stored within Defendant’s information network, including, upon information and belief, names, Social Security numbers, and driver’s license numbers (these types of information, *inter alia*, being thereafter referred to, collectively, as “personally identifiable information” or “PII”).¹ All such information is referred to in the aggregate herein as “Private Information.”

¹ Personally identifiable information (“PII”) generally incorporates information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver’s license numbers, financial account numbers, etc.).

2. With this action, Representative Plaintiffs seek to hold Defendant responsible for the harms it caused and will continue to cause Representative Plaintiffs and thousands of other similarly situated persons in the massive and preventable cyberattack purportedly experienced by Defendant on or about January 25, 2026, by which cybercriminals infiltrated Defendant's inadequately protected network and accessed the Private Information which was being kept there (the "Data Breach").

3. While Defendant claims to have discovered the breach "recently" without providing an exact date, Defendant did not begin informing victims of the Data Breach until April 15, 2026. Indeed, Representative Plaintiffs and Class Members were wholly unaware of the Data Breach until they received letters from Defendant informing them of it. The Notice received by Representative Plaintiffs was dated April 15, 2026.

4. According to multiple online reports, the Data Breach was perpetrated by notorious cybercriminal group "DragonForce".²

5. DragonForce is a Ransomware-as-a-Service group that was first observed in 2023, and "operates a multi-extortion model, with victims threatened with data leakage via the group's data leak sites, alongside reputational damage."³ Defendant knew or should have known of the tactics cybercriminal gangs like DragonForce use.

6. On February 1, 2026, DragonForce claimed credit for this breach on its leak page, stating that it had exfiltrated at least 294.65 GB of data from Defendant.⁴ Worse, DragonForce provided a link to "Publicated files", which provides access to a shocking amount of information

² <https://www.hookphish.com/blog/ransomware-group-dragonforce-hits-mullinaxford/> (last visited May 22, 2026); <https://www.breachsense.com/breaches/mullinaxford-data-breach/> (last visited May 22, 2026).

³ <https://www.sentinelone.com/blog/dragonforce-ransomware-gang-from-hacktivists-to-high-street-extortionists/> (last visited May 22, 2026).

⁴ <https://www.ransomware.live/id/TXVsbGluYXggRm9yZEBkcmFnb25mb3JjZQ==> (last visited May 22, 2026).

stolen by DragonForce in the Data Breach, including, on information and belief, Representative Plaintiffs' and the Class's Private Information under a variety of tabs including but not limited to 'sales' and 'users'.⁵

7. Thus, on information and belief, Representative Plaintiffs' and the Class's stolen Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web. Indeed, this is the *modus operandi* of cybercriminals, including DragonForce.

8. Defendant acquired, collected and stored Representative Plaintiffs' and Class Members' Private Information. Therefore, at all relevant times, Defendant knew or should have known that Representative Plaintiffs and Class Members would use Defendant's services to store and/or share sensitive data, including highly confidential Private Information.

9. Defendant disregarded the rights of Representative Plaintiffs and Class Members by intentionally, willfully, recklessly and/or negligently failing to take and implement adequate and reasonable measures to ensure that Representative Plaintiffs' and Class Members' Private Information was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, Representative Plaintiffs' and Class Members' Private Information was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party seeking to profit off this disclosure by defrauding Representative Plaintiffs and Class Members in the future. Representative Plaintiffs and Class Members have a continuing interest in ensuring their information is and remains safe and are entitled to injunctive and other equitable relief.

⁵ *Id.*

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over Representative Plaintiffs' claims under Florida Stat. § 26.012 and § 86.011. This Court has jurisdiction over this dispute because this complaint seeks damages in excess of \$50,000.00, exclusive of interest and attorneys' fees.

11. This Court has personal jurisdiction over Defendant under Florida Stat. § 48.193 because its principal address is in Florida, it regularly conducts business in Florida, and has sufficient minimum contacts in Florida.

12. Venue is proper in this forum pursuant to Florida Statute § 47.011, *et seq.* because the transactions out of which the causes of action arose occurred in Orange County.

REPRESENTATIVE PLAINTIFFS

Representative Plaintiff Debra Marino

13. Representative Plaintiff Marino is an adult individual and, at all relevant times herein, was a resident and citizen of the State of Florida. Representative Plaintiff Marino is a victim of the Data Breach.

14. Defendant received highly sensitive Private Information from Representative Plaintiff Marino in connection with the goods/services/employment Representative Plaintiff Marino obtained from Defendant. As a result, Representative Plaintiff Marino's information was among the data accessed by an unauthorized third party in the Data Breach.

15. At all times herein relevant, Representative Plaintiff Marino is and was a member of the Class.

16. Representative Plaintiff Marino's Private Information was exposed in the Data Breach because Defendant stored and/or shared Representative Plaintiff Marino's Private

Information. Representative Plaintiff Marino's Private Information was within the possession and control of Defendant at the time of the Data Breach.

17. Representative Plaintiff Marino received a letter from Defendant stating Representative Plaintiff Marino's Private Information was involved in the Data Breach (the "Notice").

18. As a result, Representative Plaintiff Marino spent time dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring Representative Plaintiff Marino's accounts and seeking legal counsel regarding Representative Plaintiff Marino's options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

19. Representative Plaintiff Marino suffered actual injury in the form of damages to and diminution in the value of Representative Plaintiff Marino's Private Information—a form of intangible property that Representative Plaintiff Marino entrusted to Defendant, which was compromised in and as a result of the Data Breach.

20. Representative Plaintiff Marino suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Representative Plaintiff Marino's Private Information.

21. Representative Plaintiff Marino suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from Representative Plaintiff Marino's Private Information being placed in the hands of unauthorized third parties/criminals.

Representative Plaintiff Marino has a continuing interest in ensuring that Representative Plaintiff Marino's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Representative Plaintiff Myra Reames-Clevenger

22. Representative Plaintiff Reames-Clevenger is an adult individual and, at all relevant times herein, was a resident and citizen of the State of Washington. Representative Plaintiff Reames-Clevenger is a victim of the Data Breach.

23. Defendant received highly sensitive Private Information from Representative Plaintiff Reames-Clevenger in connection with the services Representative Plaintiff Reames-Clevenger obtained from Defendant. As a result, Representative Plaintiff Reames-Clevenger's information was among the data accessed by an unauthorized third party in the Data Breach.

24. At all times herein relevant, Representative Plaintiff Reames-Clevenger is and was a member of the Class.

25. Representative Plaintiff Reames-Clevenger's Private Information was exposed in the Data Breach because Defendant stored and/or shared Representative Plaintiff Reames-Clevenger's Private Information. Representative Plaintiff Reames-Clevenger's Private Information was within the possession and control of Defendant at the time of the Data Breach.

26. Representative Plaintiff Reames-Clevenger provided her Private Information to Defendant and trusted that it would use reasonable measures to protect it according to state and federal law.

27. Defendant deprived Representative Plaintiff Reames-Clevenger of the earliest opportunity to guard herself against the Data Breach's effects by failing to timely notify her of the Breach.

28. As a result of their inadequate cybersecurity, Defendant exposed Representative Plaintiff Reames-Clevenger's Private Information for theft by cybercriminals and fraudsters and sale on the dark web.

29. Representative Plaintiff Reames-Clevenger spent time dealing with the consequences of the Data Breach, which includes time spent gathering information about the Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred, and dealing with spam. This time has been lost forever and cannot be recaptured.

30. Following the Data Breach, Representative Plaintiff Reames-Clevenger has experienced a large influx of spam and scam calls and emails related to car warranties and vehicle information. This further demonstrates that Representative Plaintiff Reames-Clevenger's information stolen in the Data Breach has been placed in the hands of cybercriminals.

31. Once an individual's Private Information is for sale and access on the dark web, as Representative Plaintiff Reames-Clevenger's Private Information is here as a result of the Breach, cybercriminals are able to use the stolen and compromised information to gather and steal even more information.⁶ On information and belief, the spam calls and emails Representative Plaintiff Reames-Clevenger is experiencing are a result of the Data Breach. This is consistent with the fact that, as part of receiving Defendant's services, Representative Plaintiff Reames-Clevenger provided Defendant with her contact information, including the same cell phone number and email address that is receiving increased spam.

32. Representative Plaintiff Reames-Clevenger has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Representative

⁶ What do Hackers do with Stolen Information, Aura, <https://www.aura.com/learn/what-do-hackers-do-with-stolen-information> (last visited May 22, 2026).

Plaintiff fears for her personal financial security and uncertainty over what Private Information was exposed in the Data Breach.

33. Representative Plaintiff Reames-Clevenger has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

34. Representative Plaintiff Reames-Clevenger has suffered additional actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Representative Plaintiff Reames-Clevenger entrusted to Defendant, which was compromised in and as a result of the Data Breach.

35. Representative Plaintiff Reames-Clevenger suffered actual injury from the exposure of her Private Information—which violates her rights to privacy.

36. Representative Plaintiff Reames-Clevenger has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of unauthorized third parties and possibly criminals.

37. Representative Plaintiff Reames-Clevenger has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

38. Defendant has made no statements, assurances, or acknowledgements about what concrete steps or changes it will take to prevent further unauthorized access into its systems. Representative Plaintiff Reames-Clevenger is therefore at continuing risk of future fraud, identity theft, and misuse of her Private Information as a result of the infamous cyberhacker, DragonForce,

being able to access and pilfer Defendant's systems whenever it wants and for however long it pleases.

Representative Plaintiff Shirley Rohr

39. Representative Plaintiff Rohr is an adult individual and, at all relevant times herein, was a resident and citizen of the State of Washington. Representative Plaintiff Rohr is a victim of the Data Breach.

40. Defendant received highly sensitive Private Information from Representative Plaintiff Rohr in connection with the services Representative Plaintiff Rohr obtained from Defendant. As a result, Representative Plaintiff Rohr's information was among the data accessed by an unauthorized third party in the Data Breach.

41. At all times herein relevant, Representative Plaintiff Rohr is and was a member of the Class.

42. Representative Plaintiff Rohr's Private Information was exposed in the Data Breach because Defendant stored and/or shared Representative Plaintiff Rohr's Private Information. Representative Plaintiff Rohr's Private Information was within the possession and control of Defendant at the time of the Data Breach.

43. Representative Plaintiff Rohr provided her Private Information to Defendant and trusted that it would use reasonable measures to protect it according to state and federal law.

44. Defendant deprived Representative Plaintiff Rohr of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her of the Breach.

45. As a result of its inadequate cybersecurity, Defendant exposed Representative Plaintiff Rohr's Private Information for theft by cybercriminals and fraudsters and sale on the dark web.

46. Representative Plaintiff Rohr spent time dealing with the consequences of the Data Breach, which includes time spent gathering information about the Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred, and dealing with spam. This time has been lost forever and cannot be recaptured.

47. Following the Data Breach, Representative Plaintiff Rohr has experienced a large influx of spam and scam calls and text messages. This further demonstrates that Representative Plaintiff Rohr's information stolen in the Data Breach has been placed in the hands of cybercriminals.

48. Once an individual's Private Information is for sale and access on the dark web, as Representative Plaintiff Rohr's Private Information is here as a result of the Breach, cybercriminals are able to use the stolen and compromised information to gather and steal even more information.⁷ On information and belief, the spam calls and messages Representative Plaintiff Rohr is experiencing are a result of the Data Breach. This is consistent with the fact that, as part of receiving Defendant's services, Representative Plaintiff Rohr provided Defendant with her contact information, including the same cell phone number and email address that is receiving increased spam.

49. Representative Plaintiff Rohr has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Representative Plaintiff Rohr fears for her personal financial security and uncertainty over what Private Information was exposed in the Data Breach.

50. Representative Plaintiff Rohr has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond

⁷ *Id.*

allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

51. Representative Plaintiff Rohr has suffered additional actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Representative Plaintiff Rohr entrusted to Defendant, which was compromised in and as a result of the Data Breach.

52. Representative Plaintiff Rohr suffered actual injury from the exposure of her Private Information—which violates her rights to privacy.

53. Representative Plaintiff Rohr has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of unauthorized third parties and possibly criminals.

54. Representative Plaintiff Rohr has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

55. Defendant has made no statements, assurances, or acknowledgements about what concrete steps or changes it will take to prevent further unauthorized access into its systems. Representative Plaintiff Rohr is therefore at continuing risk of future fraud, identity theft, and misuse of her Private Information as a result of the infamous cyberhacker, DragonForce, being able to access and pilfer Defendant's systems whenever it wants and for however long it pleases.

DEFENDANT

56. Defendant is a for-profit enterprise with a principal place of business located in Apopka, Florida. Defendant is a car dealership that sells new and used cars and services cars.⁸

⁸ <https://mullinaxfordfl.com/general-contact> (last accessed May 22, 2026).

57. The true names and capacities of persons or entities, whether individual, corporate, associate or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Representative Plaintiffs. Representative Plaintiffs will seek leave of court to amend this Complaint to reflect the true names and capacities of such responsible parties when their identities become known.

CLASS ACTION ALLEGATIONS

58. Representative Plaintiffs bring this action pursuant to the provisions of Rule 1.220 of the Florida Rules of Civil Procedure, on behalf of Representative Plaintiffs and the following Class (the “Class”):

All United States citizens whose Private Information was compromised in the Data Breach discovered by Defendant in February 2026, including all those who received notice of the Breach.

59. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant’s parents, subsidiaries, affiliates, officers and directors and any entity in which Defendant has a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including, but not limited to, its departments, agencies, divisions, bureaus, boards, sections, groups, counsel and/or subdivisions, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

60. Representative Plaintiffs reserve the right to amend or modify the class definition to achieve greater specificity, by further division into sub-classes and/or by limitation to particular issues.

61. This action has been brought and may properly be maintained as a class action under Rule 1.220 of the Florida Rules of Civil Procedure because there is a well-defined

community of interest in the litigation and membership in the proposed Class is easily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiffs Class are so numerous that joinder of all members is impractical, if not impossible. Membership in the Class will be determined by analysis of Defendant's records.

b. Commonality: Representative Plaintiffs and Class Members share a community of interest in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

- 1) Whether Defendant had a legal duty to Representative Plaintiffs and the Class to exercise due care in collecting, storing, using and/or safeguarding their Private Information;
- 2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;
- 3) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;
- 4) Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;
- 5) Whether Defendant failed to comply with its own policies and applicable laws, regulations and industry standards relating to data security;
- 6) Whether Defendant adequately, promptly and accurately informed Representative Plaintiffs and Class Members that their Private Information had been compromised;
- 7) How and when Defendant actually learned of the Data Breach;
- 8) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of Representative Plaintiffs' and Class Members' Private Information;
- 9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- 10) Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard Representative Plaintiffs' and Class Members' Private Information;
- 11) Whether Representative Plaintiffs and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct; and
- 12) Whether Representative Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

c. Typicality: Representative Plaintiffs' claims are typical of the claims of the Plaintiffs Class. Representative Plaintiffs and all members of the Plaintiffs

Class sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

- d. Adequacy of Representation: Representative Plaintiffs in this class action are adequate representatives of the Plaintiffs Class in that the Representative Plaintiffs have the same interest in the litigation of this case as the Class Members, are committed to vigorous prosecution of this case and have retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiffs are not subject to any individual defenses unique from those conceivably applicable to other Class Members or the Class in their entirety. Representative Plaintiffs anticipate no management difficulties in this litigation.
- e. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Plaintiffs Class to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought by each individual member of the Plaintiffs Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

62. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, such that it is impracticable to bring all Class Members before the Court.

63. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly and Representative Plaintiffs' challenge of these policies and practices hinges on Defendant's conduct with respect to the Class in its entirety, not on facts or law applicable only to Representative Plaintiffs.

64. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

65. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

COMMON FACTUAL ALLEGATIONS

The Cyberattack

66. In the course of the Data Breach, one or more unauthorized third parties accessed Class Members' Private Information. Representative Plaintiffs were among the individuals whose data was accessed in the Data Breach.

67. According to the Data Breach Notice and/or publicly filed documents, Representative Plaintiffs state, on information and belief, that thousands of persons were affected by the Data Breach.

68. Representative Plaintiffs were provided the information detailed above upon Representative Plaintiffs' receipt of a letter from Defendant. Representative Plaintiffs were not aware of the Data Breach until receiving that letter.

69. According to multiple online reports, the Data Breach was perpetrated by notorious cybercriminal group "DragonForce".⁹

70. DragonForce is a Ransomware-as-a-Service group that was first observed in 2023, and "operates a multi-extortion model, with victims threatened with data leakage via the group's

⁹ <https://www.hookphish.com/blog/ransomware-group-dragonforce-hits-mullinaxford/> (last visited May 22, 2026); <https://www.breachsense.com/breaches/mullinaxford-data-breach/> (last visited May 22, 2026).

data leak sites, alongside reputational damage.”¹⁰ Defendant knew or should have known of the tactics cybercriminal gangs like DragonForce use.

71. On February 1, 2026, DragonForce claimed credit for this breach on its leak page, stating that it had exfiltrated at least 294.65 GB of data from Defendant.¹¹ Worse, DragonForce provided a link to “Publicated files”, which provides access to a shocking amount of information stolen by DragonForce in the Data Breach, including, on information and belief, Representative Plaintiffs’ and the Class’s Private Information under a variety of tabs including but not limited to ‘sales’ and ‘users’.¹²

72. Thus, on information and belief, Representative Plaintiffs’ and the Class’s stolen Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web. Indeed, this is the *modus operandi* of cybercriminals, including DragonForce.

Defendant’s Failed Response to the Breach

73. Upon information and belief, the unauthorized third-party cybercriminals gained access to Representative Plaintiffs’ and Class Members’ Private Information with the intent of misusing the Private Information, including marketing and selling Representative Plaintiffs’ and Class Members’ Private Information.

74. Not until long after it claims to have discovered the Data Breach did Defendant begin sending the Notice to persons whose Private Information Defendant confirmed was

¹⁰ <https://www.sentinelone.com/blog/dragonforce-ransomware-gang-from-hacktivists-to-high-street-extortionists/> (last visited May 22, 2026).

¹¹ <https://www.ransomware.live/id/TXVsbGluYXggRm9yZEBkcmFnbn25mb3JjZQ==> (last visited May 22, 2026).

¹² *Id.*

potentially compromised as a result of the Data Breach. The Notice provided basic details of the Data Breach and Defendant's recommended next steps.

75. Representative Plaintiffs and Class Members were required to provide their Private Information to Defendant in order to receive services from Defendant. Thus, Defendant created, collected and stored Representative Plaintiffs' and Class Members' Private Information with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

76. Despite this, Representative Plaintiffs and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used and what steps are being taken, if any, to secure their Private Information going forward. Representative Plaintiffs and Class Members are thus left to speculate as to where their Private Information ended up, who has used it and for what potentially nefarious purposes. Indeed, they are left to further speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

77. Representative Plaintiffs' and Class Members' Private Information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed Private Information for targeted marketing without Representative Plaintiffs' and/or Class Members' approval. Either way, unauthorized individuals can now easily access Representative Plaintiffs' and Class Members' Private Information.

Defendant Collected/Stored Class Members' Private Information

78. Defendant acquired, collected, stored and assured reasonable security over Representative Plaintiffs' and Class Members' Private Information.

79. As a condition of its relationships with Representative Plaintiffs and Class Members, Defendant required that Representative Plaintiffs and Class Members entrust Defendant with highly sensitive and confidential Private Information. Defendant, in turn, stored that information on Defendant's system that was ultimately affected by the Data Breach.

80. By obtaining, collecting and storing Representative Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties over the Private Information and knew or should have known that it was thereafter responsible for protecting Representative Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

81. Representative Plaintiffs and Class Members have taken reasonable steps to maintain their Private Information's confidentiality. Representative Plaintiffs and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only and to make only authorized disclosures of this information.

82. Defendant could have prevented the Data Breach by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Representative Plaintiffs' and Class Members' Private Information.

83. Defendant's negligence in safeguarding Representative Plaintiffs' and Class Members' Private Information is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

84. Due to the high-profile nature of these breaches, and other breaches of its kind, Defendant was and/or certainly should have been on notice and aware of such attacks occurring in its industry and, therefore, should have assumed and adequately performed the duty of preparing

for such an imminent attack. This is especially true given that Defendant is a large, sophisticated operation with the resources to put adequate data security protocols in place.

85. And yet, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Representative Plaintiffs' and Class Members' Private Information from being compromised.

Defendant Had an Obligation to Protect the Stolen Information

86. In failing to adequately secure Representative Plaintiffs' and Class Members' sensitive data, Defendant breached duties it owed Representative Plaintiffs and Class Members under statutory and common law.

87. Representative Plaintiffs and Class Members surrendered their highly sensitive Private Information to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their Private Information, independent of any statute.

88. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

89. In addition to its obligations under federal and state laws, Defendant owed a duty to Representative Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the Private Information in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant

owed a duty to Representative Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks and protocols adequately protected Representative Plaintiffs' and Class Members' Private Information.

90. Defendant owed a duty to Representative Plaintiffs and Class Members to design, maintain and test its computer systems, servers and networks to ensure that all Private Information in its possession was adequately secured and protected.

91. Defendant owed a duty to Representative Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect all Private Information in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

92. Defendant owed a duty to Representative Plaintiffs and Class Members to implement processes that would immediately detect a breach of its data security systems in a timely manner.

93. Defendant owed a duty to Representative Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

94. Defendant owed a duty to Representative Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' Private Information from theft because such an inadequacy would be a material fact in the decision to entrust their Private Information to Defendant.

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

96. Defendant owed a duty to Representative Plaintiffs and Class Members to encrypt and/or more reliably encrypt Representative Plaintiffs' and Class Members' Private Information and monitor user behavior and activity in order to identify possible threats.

The Data Breach Was Foreseeable and the Defendant Was Aware of Its Risk

97. It is well known that Private Information, including names and Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

98. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting institutions that collect and store Private Information, like Defendant, preceding the date of the Data Breach.

99. In 2023, a record 3,205 data breaches occurred in the United States, resulting in about 349,221,481 sensitive records being exposed, a greater than 100% increase from 2019.¹³ These statistics have held steady for 2024 – when 3,158 data compromises occurred.¹⁴

100. Individuals place a high value not only on their PII, but also on the privacy of that data. For the individual, identity theft causes significant negative financial impact on victims as well as severe distress and other strong emotions and physical reactions.

101. In light of recent high profile data breaches at other industry leading companies, including, LoanDepot (16.9 million affected, January 2024), Evolve Bank & Trust (7.6 million affected, May 2024), Financial Business and Consumer Solutions (4.2 million affected, February 2024), and Prudential Financial (2.5 million affected, February 2024) Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

¹³ ITRC (Identity Theft Resource Center), *2023 Data Breach Report* (January 2024), available at <https://www.idtheftcenter.org/post/2023-annual-data-breach-report-reveals-record-number-of-compromises-72-percent-increase-over-previous-high/> (last visited May 22, 2026).

¹⁴ ITRC (Identity Theft Resource Center), *2024 Data Breach Report* (January 2025), available at <https://www.idtheftcenter.org/publication/2024-data-breach-report/> (last visited May 22, 2026).

102. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

103. Despite the prevalence of public announcements of data breach and data security compromises, and despite their own acknowledgment of its duties to keep the Private Information private and secure, Defendant failed to take appropriate steps to protect the Private Information of Representative Plaintiffs and the proposed Class from being compromised.

Defendant Could Have Prevented the Data Breach

104. Data breaches are preventable.¹⁵ “In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions.”¹⁶ “Organizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised[.]”¹⁷

105. Most reported data breaches “are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.”¹⁸

106. Here, many failures laid the groundwork for the Data Breach.

¹⁵ Lucy L. Thomson, *Despite the Alarming Trends, Data Breaches Are Preventable*, DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012), available at <https://lawcat.berkeley.edu/record/394088>.

¹⁶ *Id.* at 17.

¹⁷ *Id.* at 28.

¹⁸ *Id.*

107. The FTC has published guidelines that establish reasonable data security practices for businesses.¹⁹

108. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.²⁰

109. The FTC guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems.²¹

110. The FTC guidelines also recommend that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.²²

111. According to information and belief, Defendant failed to follow reasonable and necessary industry standards to prevent a data breach, including the FTC's guidelines.

112. Defendant was at all times fully aware of its obligation to protect the Private Information of consumers under the FTCA, yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored, and the foreseeable consequences of the immense damages that would result to Representative Plaintiffs and the Class.

¹⁹ *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

²⁰ *Id.*

²¹ *Id.*

²² *Id.*

113. Based on allowing its security certificates to lapse and upon information and belief, Defendant also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in cybersecurity readiness.

114. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”²³

115. To prevent and detect the attack here, Defendant could and should have taken, as recommended by the Federal Bureau of Investigation, the following measures:

- Implemented an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enabled strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scanned all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configured firewalls to block access to known malicious IP addresses.
- Patched operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Managed the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and

²³ See *How to Protect Your Networks from RANSOMWARE*, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>.

those with a need for administrator accounts should only use them when necessary.

- Configured access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disabled macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implemented Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Considered disabling Remote Desktop protocol (RDP) if it is not being used.
- Used application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Executed operating system environments or specific programs in a virtualized environment.
- Categorized data based on organizational value and implement physical and logical separation of networks and data for different organizational units.²⁴

116. According to information and belief, Defendant failed to do any of the above.

117. To prevent and detect cyberattacks, Defendant could and should have recommended its employees, as recommended by the United States Cybersecurity & Infrastructure Security Agency, take the following measures:

- **Updated and patched your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.
- **Used caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender

²⁴ *Id.* at 3–4.

organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net).

- **Opened email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Kept your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it.
- **Verified email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Used and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.²⁵

118. In addition, to prevent and detect the Data Breach Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Harden internet-facing assets**
 - Apply latest security updates
 - Use threat and vulnerability management
 - Perform regular audits

²⁵ See *Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (revised Sept. 2, 2021), <https://www.cisa.gov/news-events/news/protecting-against-ransomware> (internal citations omitted).

- **Thoroughly investigate and remediate alerts.**
 - Prioritize and treat commodity malware infections as potential full compromise of the system
- **Include IT professionals in security discussions.**
 - Ensure collaboration among security operations, security administrators, and information technology administrators to configure servers and other endpoints securely
- **Build and maintain credential hygiene**
 - Use multifactor authentication or network level authentication and enforce strong, randomized, just-in-time local administrator passwords
- **Apply principle of least-privilege**
 - Monitor for adversarial activities
 - Hunt for brute force attempts
 - Monitor for cleanup of Event Logs
 - Analyze logon events
- **Harden infrastructure**
 - Utilize Windows Defender Firewall
 - Enable tamper protection
 - Enable cloud-delivered protection
 - Turn on attack surface reduction rules and Antimalware Scan Interface for Office Visual Basic for Applications²⁶

119. Specifically, among other failures, Defendant had far too much confidential unencrypted information held on its systems. Such Private Information should have been segregated into an encrypted system.²⁷

²⁶ See *Human-operated ransomware attacks: A preventable disaster*, MICROSOFT THREAT INTELLIGENCE (Mar 5, 2020), <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>.

²⁷ See Adnan Raja, *How to Safeguard Your Business Data With Encryption*, DATAINSIDER (Aug. 14, 2018), <https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption>.

120. Moreover, it is well-established industry standard practice for a business to dispose of confidential Private Information once it is no longer needed.²⁸

121. The FTC has repeatedly emphasized the importance of disposing of unnecessary Private Information: “Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it’s not on your system, it can’t be stolen by hackers.”²⁹ Rather than following this basic standard of care, Defendant kept thousands of individuals’ unencrypted Private Information on their inadequately secured systems indefinitely.

122. In sum, the Data Breach could have been easily prevented through standard practices like the use of industry standard network segmentation, redaction, and encryption of all Private Information—which Defendant negligently failed to do.

123. Further, the scope of the Data Breach could have been dramatically reduced had Defendant utilized proper record retention and destruction practices—but Defendant negligently did no such thing.

Value of the Relevant Sensitive Information

124. While the greater efficiency of electronic records translates to cost savings for providers, it also comes with the risk of privacy breaches. These electronic records contain a plethora of sensitive information that is valuable to cybercriminals. In the retail or employment context, for example, one customer’s or employee’s complete record can be sold for hundreds of dollars on the dark web. As such, Private Information is a valuable commodity for which a “cyber

²⁸ See *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business>.

²⁹ *Id.* at 6.

black market” exists in which criminals openly post stolen payment card numbers, Social Security numbers and other personal information on a number of underground internet websites.

125. The high value of Private Information to criminals is further evidenced by the prices they will pay for it through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.³⁰ Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.³¹ Criminals can also purchase access to entire company data breaches from \$999 to \$4,995.³²

126. These criminal activities have and will result in devastating financial and personal losses to Representative Plaintiffs and Class Members. For example, it is believed that certain Private Information compromised in the 2017 Equifax data breach was being used three years later by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Representative Plaintiffs and Class Members for the rest of their lives. They will need to remain constantly vigilant.

127. The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” 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,

³⁰ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>

³¹ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>.

³² *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>.

alien registration number, government passport number, employer or taxpayer identification number.”

128. Identity thieves can use Private Information, such as that of Representative Plaintiffs and Class Members which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver’s license or identification card in the victim’s name but with another’s picture, using the victim’s information to obtain government benefits or filing a fraudulent tax return using the victim’s information to obtain a fraudulent refund.

129. The ramifications of Defendant’s failure to keep secure Representative Plaintiffs’ and Class Members’ Private Information are long lasting and severe. Once Private Information is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, Representative Plaintiffs’ and Class Members’ Private Information was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the Private Information for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

130. There may be a time lag between when harm occurs versus when it is discovered and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[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.³³

³³ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <http://www.gao.gov/new.items/d07737.pdf/>.

131. And data breaches are preventable.³⁴ As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, “[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions.”³⁵ She added that “[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised....”³⁶

132. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules and procedures. Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.³⁷

133. Here, Defendant knew of the importance of safeguarding Private Information and of the foreseeable consequences that would occur if Representative Plaintiffs’ and Class Members’ Private Information was stolen, including the significant costs that would be placed on Representative Plaintiffs and Class Members as a result of a breach of this magnitude. As detailed above, Defendant knew or should have known that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Representative Plaintiffs and Class Members. Its failure to do so is therefore intentional, willful, reckless and/or grossly negligent.

134. Defendant disregarded the rights of Representative Plaintiffs and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly and/or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized

³⁴ Lucy L. Thompson, “Despite the Alarming Trends, Data Breaches Are Preventable,” in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

³⁵ *Id.* at 17.

³⁶ *Id.* at 28.

³⁷ *Id.*

intrusions, (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Representative Plaintiffs’ and Class Members’ Private Information, (iii) failing to take standard and reasonably available steps to prevent the Data Breach, (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time, and (v) failing to provide Representative Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

The Harm Caused by the Data Breach Now and Going Forward

135. Victims of data breaches are susceptible to becoming victims of identity theft for years to come. The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” 17 C.F.R. § 248.201(9).

136. The type of data that may have been accessed and compromised here can be used to perpetrate fraud and identity theft and Representative Plaintiffs and Class Members face a substantial risk of identity theft given that their Private Information was compromised in the Data Breach.

137. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, the stolen information often ends up on the dark web, where malicious actors buy and sell that information for profit.³⁸

138. For example, when the U.S. Department of Justice announced their seizure of AlphaBay—the largest online “dark market”—in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another

³⁸ *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Dec. 28, 2020) <https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring> (last visited May 22, 2026).

person's identity.”³⁹ Marketplaces similar to the now-defunct AlphaBay continue to be “awash with [PII] belonging to victims from countries all over the world.”⁴⁰

139. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft-related crimes discussed below.

140. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

141. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as “social engineering” to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches can be the starting point for these additional targeted attacks on the victim.

142. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of “Fullz” packages.⁴¹

³⁹ *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (April 3, 2018) <https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/> (last visited May 22, 2026).

⁴⁰ *Id.*

⁴¹ “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that

143. With “Fullz” packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

144. The development of “Fullz” packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Representative Plaintiffs’ and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information, such as emails, phone numbers, or credit card numbers, may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

145. According to the FBI’s Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, “rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good.”⁴² Defendant did not rapidly report to Representative Plaintiffs and

can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), <https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/>. (last visited May 22, 2026).

⁴² 2019 Internet Crime Report Released, FBI (Feb. 11, 2020) <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion> (last visited May 22, 2026).

Class Members that their Private Information had been stolen. Defendant did not notify impacted people for seven months after learning of the Data Breach.

146. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the resource and asset of time has been lost.

147. Representative Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

148. These efforts are consistent with the U.S. Government Accountability Office, which released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”⁴³

149. These efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended

⁴³ See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>. (last visited May 22, 2026).

fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.⁴⁴

Diminution of Value of PII

150. PII is a valuable property right.⁴⁵ The value is axiomatic, considering the value of Big Data in corporate America, and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates beyond a doubt that Private Information has considerable market value.

151. As a result of the Data Breach, Representative Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Representative Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

152. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Representative Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Representative Plaintiffs and Class Members as a result of a breach.

⁴⁴ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps>. (last visited May 22, 2026).

⁴⁵ See, e.g., Randall T. Soma, et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted). (last visited May 22, 2026).

153. As a result of the Data Breach, the Private Information of Representative Plaintiffs and Class Members has been exposed to criminals for misuse. The injuries suffered by Representative Plaintiffs and Class Members, or likely to be suffered as a direct result of Defendant's Data Breach, include: (a) theft of their Private Information; (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 ameliorate, mitigate, and deal with the consequences of this Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard their Private Information against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further injurious breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Representative Plaintiffs' and Class Members' Private Information.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

154. In addition to a remedy for economic harm, Representative Plaintiffs and Class Members maintain an interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

155. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, there is

a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes.

156. Such fraud may go undetected for years; consequently, Representative Plaintiffs and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

157. As a result, Representative Plaintiffs and Class Members also request relief in the form of the future cost of credit and identity theft monitoring, which is reasonable and necessary. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from the Data Breach.

Loss of the Benefit of the Bargain

158. Furthermore, Defendant's poor data security deprived Representative Plaintiffs and Class Members of the benefit of their bargain. When agreeing to directly or indirectly provide their Private Information to Defendant, Representative Plaintiffs and other reasonable consumers understood and expected that in exchange, Defendant would implement necessary data security to protect the Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Representative Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

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

159. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

160. At all times herein relevant, Defendant owed Representative Plaintiffs and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their Private Information and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing Representative Plaintiffs' and Class Members' Private Information on its computer systems and networks.

161. Among these duties, Defendant was expected:

- a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the Private Information in its possession;
- b. to protect Representative Plaintiffs' and Class Members' Private Information using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;
- c. to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches; and
- d. to promptly notify Representative Plaintiffs and Class Members of any data breach, security incident or intrusion that affected or may have affected their Private Information.

162. Defendant knew that the Private Information was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Representative Plaintiffs and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

163. Defendant knew or should have known of the risks inherent in collecting and storing Private Information, the vulnerabilities of its data security systems and the importance of adequate security. Defendant knew about numerous, well-publicized data breaches.

164. Defendant knew or should have known that its data systems and networks did not adequately safeguard Representative Plaintiffs' and Class Members' Private Information.

165. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the Private Information that Representative Plaintiffs and Class Members had entrusted to it.

166. Defendant breached its duties to Representative Plaintiffs and Class Members by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Representative Plaintiffs' and Class Members' Private Information.

167. Because Defendant knew that a breach of its systems could damage thousands of individuals, including Representative Plaintiffs and Class Members, Defendant had a duty to adequately protect its data systems and the Private Information contained thereon.

168. Representative Plaintiffs' and Class Members' willingness to entrust Defendant with its Private Information was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the Private Information it stored on them from attack. Thus, Defendant had a special relationship with Representative Plaintiffs and Class Members.

169. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Representative Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant and Representative Plaintiffs and/or the remaining Class Members.

170. Defendant breached its general duty of care to Representative Plaintiffs and Class Members in, but not necessarily limited to, the following ways:

- a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Representative Plaintiffs' and Class Members' Private Information;
- b. by failing to timely and accurately disclose that Representative Plaintiffs' and Class Members' Private Information had been improperly acquired or accessed;
- c. by failing to adequately protect and safeguard the Private Information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information;

- d. by failing to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Representative Plaintiffs' and Class Members' Private Information, misuse the Private Information and intentionally disclose it to others without consent;
- e. by failing to adequately train its employees to not store Private Information longer than absolutely necessary;
- f. by failing to consistently enforce security policies aimed at protecting Representative Plaintiffs' and the Class Members' Private Information;
- g. by failing to implement processes to quickly detect data breaches, security incidents or intrusions; and
- h. by failing to encrypt Representative Plaintiffs' and Class Members' Private Information and monitor user behavior and activity in order to identify possible threats.

171. Defendant's willful failure to abide by these duties was wrongful, reckless and/or grossly negligent in light of the foreseeable risks and known threats.

172. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Representative Plaintiffs and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

173. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the Private Information to Representative Plaintiffs and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their Private Information.

174. Defendant breached its duty to notify Representative Plaintiffs and Class Members of the unauthorized access by waiting almost a year after learning of the Data Breach to notify Representative Plaintiffs and Class Members and then by failing and continuing to fail to provide Representative Plaintiffs and Class Members sufficient information regarding the breach. To date, Defendant has not provided sufficient information to Representative Plaintiffs and Class Members

regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Representative Plaintiffs and Class Members.

175. Further, through its failure to provide timely and clear notification of the Data Breach to Representative Plaintiffs and Class Members, Defendant prevented Representative Plaintiffs and Class Members from taking meaningful, proactive steps to, *inter alia*, secure and/or access their Private Information.

176. There is a close causal connection between Defendant's failure to implement security measures to protect Representative Plaintiffs' and Class Members' Private Information and the harm suffered, or risk of imminent harm suffered, by Representative Plaintiffs and Class Members. Representative Plaintiffs' and Class Members' Private Information was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing and maintaining appropriate security measures.

177. Defendant's wrongful actions, inactions and omissions constituted (and continue to constitute) common law negligence.

178. The damages Representative Plaintiffs and Class Members have suffered (as alleged above) and will continue to suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

179. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits "unfair [...] practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

180. Defendant violated 15 U.S.C. § 45 by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Representative Plaintiffs and Class Members.

181. Defendant's violation of 15 U.S.C. § 45 constitutes negligence *per se*.

182. As a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will continue to suffer injury, including, but not limited to (i) actual identity theft, (ii) the loss of the opportunity of how their Private Information is used, (iii) the compromise, publication and/or theft of their Private Information, (iv) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft, tax fraud and/or unauthorized use of their Private Information, (v) 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 embarrassment and identity theft, (vi) lost continuity in relation to their personal records, (vii) the continued risk to their Private Information, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Representative Plaintiffs' and Class Members' Private Information 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 impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Representative Plaintiffs and Class Members.

183. As a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy and other economic and noneconomic losses.

184. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiffs and Class Members have suffered and will continue to suffer the continued risks of exposure of their Private Information, 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 Private Information in its continued possession.

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

185. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

186. Through their course of conduct, Defendant, Representative Plaintiffs and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Representative Plaintiffs' and Class Members' Private Information.

187. Defendant solicited, invited and required Representative Plaintiffs and Class Members to provide their Private Information as part of Defendant's regular business practices. Representative Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

188. As a condition of being direct customers and/or employees of Defendant, Representative Plaintiffs and Class Members provided and entrusted their Private Information to

Defendant. In so doing, Representative Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential and to timely and accurately notify Representative Plaintiffs and Class Members if its data had been breached and compromised or stolen.

189. A meeting of the minds occurred when Representative Plaintiffs and Class Members agreed to, and did, provide their Private Information to Defendant, in exchange for, amongst other things, the protection of their Private Information.

190. Representative Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

191. Defendant breached the implied contracts it made with Representative Plaintiffs and Class Members by failing to safeguard and protect their Private Information and by failing to provide timely and accurate notice to them that their Private Information was compromised as a result of the Data Breach.

192. As a direct and proximate result of Defendant's above-described breach of implied contract, Representative Plaintiffs and Class Members have suffered and will continue to suffer (i) ongoing, imminent and impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (ii) actual identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (iii) loss of the confidentiality of the stolen confidential data, (iv) the illegal sale of the compromised data on the dark web, (v) lost work time, and (f) other economic and noneconomic harm.

THIRD CAUSE OF ACTION
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of Representative Plaintiffs and the Class)

193. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth therein.

194. Every contract in this State has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

195. Representative Plaintiffs and Class Members have complied with and performed all conditions of their contracts with Defendant.

196. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Representative Plaintiffs and Class Members and continued acceptance of Private Information and storage of other personal information after Defendant knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach.

197. Defendant acted in bad faith and/or with malicious motive in denying Representative Plaintiffs and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

RELIEF SOUGHT

WHEREFORE, Representative Plaintiffs, on Representative Plaintiffs' own behalf and on behalf of each member of the proposed Class, respectfully requests that the Court enter judgment in Representative Plaintiffs' favor and for the following specific relief against Defendant (and/or each of them) as follows:

1. That the Court declare, adjudge and decree that this action is a proper class action and certify each of the proposed Class and/or any other appropriate subclasses under Rule 1.220

of the Florida Rules of Civil Procedure, including appointment of Representative Plaintiffs' counsel as Class Counsel;

2. For an award of damages, including actual, nominal and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendant, ordering it to cease and desist from unlawful activities;

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

5. For injunctive relief requested by Representative Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Representative Plaintiffs and Class Members, including, but not limited to, an Order:

- a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
- b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards and federal, state or local laws;
- c. requiring Defendant to delete and purge Representative Plaintiffs' and Class Members' Private Information unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Representative Plaintiffs and Class Members;
- d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Representative Plaintiffs' and Class Members' Private Information;
- e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests and audits on Defendant's systems on a periodic basis;
- f. prohibiting Defendant from maintaining Representative Plaintiffs' and Class Members' Private Information on a cloud-based database;

- g. requiring Defendant to segment data by creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
 - h. requiring Defendant to conduct regular database scanning and security checks;
 - i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Private Information, as well as protecting the Private Information of Representative Plaintiffs and Class Members;
 - j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs and systems for protecting personal identifying information;
 - k. requiring Defendant to implement, maintain, review and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested and updated; and
 - l. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.
- 6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;
 - 7. For an award of attorneys' fees, costs and litigation expenses, as allowed by law;
- and
- 8. For all other Orders, findings and determinations identified and sought in this Complaint.

JURY DEMAND

Representative Plaintiffs, individually and on behalf of the Class, hereby demand a trial by jury for all issues triable by jury.

Dated: June 2, 2026

By: /s/ Tonyia Johnson
Tonyia Johnson (FBN 1058251)
SHAMIS & GENTILE, P.A.

14 NE 1st Ave, Suite 705
Miami, FL 33132
Tel: (305) 479-2299
tjohnson@shamisgentile.com

Cortney Beth Szaran, Esq. (FL S.B. #1033486)
Laura Van Note, Esq. (CA S.D. #310160)*
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
Tel: (510) 891-9800
Fax: (510) 891-7030
cbs@colevannote.com
lvn@colevannote.com

Carolyn Chen*
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
Tel: (872) 273-1100
Fax: (872) 263-1109
cchen@straussborrelli.com

*Attorneys for Representative Plaintiffs
and the Class*

* *pro hac vice* forthcoming