UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF LOUISIANA

KEVIN MERRELL	**CIVIL ACTION**
VERSUS	**NO. 23-1450**
1ST LAKE PROPERTIES, INC.	**SECTION: "R"(2)**

FIRST AMENDED COMPLAINT

TABLE OF CONTENTS

NOW INTO COURT, through undersigned counsel, comes Plaintiff, Kevin Merrell ("Plaintiff"), who brings this First Amended Complaint individually, and as a representative of a putative class of persons similarly situation, and respectfully represent the following:

I. PARTIES

1. Plaintiff herein, individually, and as a representative of a putative class of persons similarly situation, is Kevin Merrell. Plaintiff is a person of the full age of majority and domiciled in the Parish of Jefferson, State of Louisiana. Plaintiff seeks to bring this lawsuit individually and as a representative of and on behalf of all other persons similarly situation who provided their Personal Identifying Information ("PII") to 1st Lake Properties, and who had their PII breached due to 1st Lake's misconduct.

2. Defendant is 1st Lake Properties, Inc., a domestic corporation authorized to do business and is doing business in the State of Louisiana, whose domicile address is 3925 North I-10 Service Road West, Metairie, Louisiana 70002.

II. JURISDICTION AND VENUE

3. This Court has jurisdiction over this matter because Defendant removed this action from the 24th Judicial District Court for the Parish of Jefferson on the basis that the Court had original subject matter jurisdiction under 28 U.S.C. § 1332(d). Plaintiff has not moved to remand the proceeding.

4. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1441(a) and 1446(a) as it is the District Court which embraces the 24th Judicial District Court for the Parish of Jefferson.

III. FACTUAL BACKGROUND

a. Defendant Collected and Stored the PII of Plaintiff and the Class

5. Defendant is a developer and property manager in the New Orleans area.[1]

6. Defendant boasts "over 9,500 apartment units in greater New Orleans, primarily in Metairie, Kenner, and River Ridge."[2] Defendant advertises that "[w]e have apartment properties throughout Southeast Louisiana in Baton Rouge and on the Northshore."[3] Also, Defendant "manages a number of suburban office buildings, neighborhood retail shopping centers, warehouses, and self-storage buildings in the New Orleans area."[4]

7. Defendant advertises that its "first and foremost goal" is to "provide an ideal living experience for our residents through exceptional customer service and a commitment to the highest standards of quality."[5]

8. In collecting and maintaining the PII, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class members themselves took reasonable steps to secure their PII.

9. As part of its business, Defendant receives and maintains the PII of thousands of its current and former tenants. In doing so, Defendant implicitly promises to safeguard their PII.

10. Under state and federal law, businesses like Defendant have duties to protect its current and former tenants' PII and to notify them about breaches.

11. Defendant recognizes these duties, declaring that:

---

[1] *About 1st Lake Properties*, 1ST LAKE, https://1stlake.com/new-orleans-apartments-1st-lake/ (last visited Mar. 16, 2023).
[2] *Id*.
[3] *Id*.
[4] *Id*.
[5] *Id*.

a. "we have put in place appropriate physical, electronic and managerial procedures reasonably designed to safeguard the information we collect;" [6] and

b. "[1st Lake] is committed to providing each of our users with a safe and satisfying experience;"[7] and

c. "We are fully committed to protecting your personal information."[8]

b. Defendant's Data Breach

12. On December 25, 2021, Defendant realized that it was hacked. But as Defendant's notice to its tenants shows, Defendant is unable—or unwilling—to determine the Data Breach's start date and/or duration.

13. Defendant states that it "issued its first round of notices" to its Data Breach victims on February 18, 2022. But Defendant's filings with the Office of the Maine Attorney General reveals that Defendant notified its Data Breach victims on July 22, 2022—approximately 209 days after Defendant discovered its Data Breach.

14. Thus, Defendant kept much of the Class in the dark—thereby depriving them of the opportunity to try and mitigate their injuries in a timely manner.

15. And when Defendant did notify Plaintiff and the Class of the Data Breach, Defendant acknowledged that their Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiff and the Class that:

d. "We recommend you take precautions."

[6] *Privacy Policy*, 1ST LAKE, https://1stlake.com/privacy-policy/ (last visited Mar. 16, 2023).
[7] *Id*.
[8] *Notice*, MAINE ATTORNEY GENERAL, https://apps.web.maine.gov/online/aeviewer/ME/40/7084c924-267d-4aa3-8483-a2b1c6e426ab.shtml (last visited Mar. 16, 2023).

e. "Freeze your credit file."

f. "Place fraud alerts on your credit file."

g. "Remain vigilant: review your account statements & report fraud."

h. "Order your free annual credit reports."

i. "Change passwords and security verification questions and answers."

j. "Obtain information about preventing identity theft, fraud alerts, security freezes and FCRA from the Federal Trade Commission."

k. "Obtain information about preventing identity theft from your state attorney general."[9]

16. Because of Defendant's Data Breach, at least the following types of PII were compromised:

a. names;

b. Social Security numbers;

c. driver's license numbers;

d. financial account numbers;

e. credit card numbers; and

f. debit card numbers.[10]

17. In total, Defendant injured thousands of people—via the exposure of their PII—in the Data Breach. Upon information and belief, these thousands of people persons include current and former tenants.

[9] *Id*.
[10] *Data Security Breach Reports*, ATTORNEY GENERAL TEXAS, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited Mar. 16, 2023).

18. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII. And thus, Defendant caused widespread injury and monetary damages. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

19. Since the breach, Defendant advertises that "1st Lake Properties is continuing to take steps to enhance its security."[11] But this is too little too late. Simply put, these steps—which Defendant now recognizes as necessary—should have been implemented before the Data Breach.

20. Defendant has done little to remedy its Data Breach. True, Defendant has offered some victims credit monitoring and insurance. But upon information and belief, such services are wholly insufficient to compensate Plaintiff and Class members for the injuries that Defendant inflicted upon them.

21. Because of Defendant's Data Breach, the sensitive PII of Plaintiff and Class members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class members.

c. Plaintiff's Experiences and Injuries

22. Plaintiff was a tenant of Defendant from approximately 2017 to 2018. As a result, Plaintiff Kevin Merrell was injured by Defendant's Data Breach.

23. As a prerequisite to becoming a tenant, Defendant required that Plaintiff disclose his PII. Thus, Defendant obtained and maintained Plaintiff's PII.

24. Plaintiff provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and

[11] *Notice*, MAINE ATTORNEY GENERAL, https://apps.web.maine.gov/online/aeviewer/ME/40/7084c924-267d-4aa3-8483-a2b1c6e426ab.shtml (last visited Mar. 16, 2023).

federal law. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

25. Plaintiff reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of PII.

26. Plaintiff does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

27. Plaintiff received a Notice of Data Breach in late 2022.

28. Through its Data Breach, Defendant compromised, upon information and belief, Plaintiff's:

a. name;

b. Social Security number;

c. driver's license number;

d. financial account numbers;

e. credit card numbers; and

f. debit card numbers.

29. Defendant's negligence inflicted a number of injuries upon Plaintiff.

30. Plaintiff received a notice in the mail from Verizon, fraudulently alleging that he purchased several devices including an iPhone, iPad, and Apple Watch—and that Plaintiff thus owed $700.Plaintiff was forced to report this fraud to Verizon and was forced to close the account with Verizon.

31. Plaintiff also received a bill from AT&T in approximately March 2023 for approximately $800 related to purchases he did not make. AT&T is requiring Plaintiff to file a police report for identity theft in order to have these charges removed.

32. Additionally, Plaintiff was subjected to an unauthorized inquiry on his credit from T-Mobile, a form of identity theft indicating that someone has fraudulently applied for lines of credit in his name.

33. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

34. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

35. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

36. Plaintiff suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

37. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

38. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII right in the hands of criminals.

39. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

40. Today, Plaintiff has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

d. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

41. Because of Defendant's failure to prevent the Data Breach, Plaintiff and Class members suffered—and will continue to suffer—damages. These damages include, inter alia, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII is used;

b. diminution in value of their PII;

c. compromise and continuing publication of their PII;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII; and

h. continued risk to their PII—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII.

42. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

43. The value of Plaintiff and Class's PII on the black market is considerable. Stolen PII trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "dark web"—further exposing the information.

44. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII far and wide.

45. One way that criminals profit from stolen PII is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

46. The development of "Fullz" packages means that the PII exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet.

47. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can 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. That is exactly what is happening to Plaintiff and Class members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class members' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

48. Defendant disclosed the PII of Plaintiff and Class members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and Class members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

49. Defendant's failure to promptly and properly notify Plaintiff and Class members of the Data Breach exacerbated Plaintiff and Class members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

e. Defendant Knew – Or Should have Known – of the Risk of a Data Breach

50. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and or data breaches in recent years.

51. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[12]

52. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[13]

---

[12] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.

[13] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

53. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

f. Defendant Failed to Follow FTC Guidelines

54. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

55. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business. There, the FTC set guidelines for what data security principles and practices businesses must use.[14] The FTC declared that, inter alia, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

56. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

57. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

[14] *Protecting Personal Information: A Guide for Business,* FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

58. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

59. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to current and former tenants' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

g. Defendant Failed to Follow Industry Standards

60. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

61. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

62. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

63. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

IV. CLASS ACTION ALLEGATIONS

64. Plaintiff seeks to have this matter proceed as a Class Action pursuant to Federal Rule of Civil Procedure 23, *et seq.,* individually and on behalf of a class of individuals similarly situated, as Plaintiff represents that he has suffered injuries and/or damages which are common to all those similarly situated who incurred injuries and/or damages arising from the tortious acts and omissions committed by Defendant 1st Lake Properties.

65. Plaintiff, Kevin Merrell, wishes to serve as a class representative to represent all other individuals similarly situated and propose that the class of individuals sought to be made Class Plaintiffs be defined as follows:

> All individuals residing in the Louisiana whose PII was compromised in the Data Breach discovered by 1st Lake Properties, Inc. in December 2021.

66. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or

director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

67. Plaintiff hereby reserves the right to amend the above class definition as necessary if further investigation and discovery reveals that the class definition should be narrowed, expanded, or otherwise modified.

68. This action is properly maintainable as a class action pursuant to F.R.C.P. 23 for the following reasons:

a. Numerosity

69. The exact number and identities of the class members are unknown at this time and may be ascertained through appropriate discovery, but upon information and belief, there are thousands of persons who had their PII compromised by the 1st Lake Properties' data breach.

70. Accordingly, and pursuant to F.R.C.P 23(a)(1) the number of individuals sought to be made class members is so numerous that joinder of all members would be impracticable.

71. Further, separate suits would only unduly burden this Judicial District and this Court, and a class action would clearly be more useful and judicially expedient than the other available procedures.

b. Commonality

72. Pursuant to F.R.C.P 23(a)(2) the questions of fact and questions of law, including defenses, presented by this litigation are and will be common to all members of the putative class described herein. These legal and factual questions predominate over any other questions affecting only individual class members, including but not limited to the following:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiff' and the Class's PII;

b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Defendant were negligent in maintaining, protecting, and securing PII;

d. if Defendant breached contract promises to safeguard Plaintiff and the Class's PII;

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiff and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

73. Plaintiff's claims asserted herein are all similar in nature and typical of the claims of each potential class member of the acts negligence, and violation of the Louisiana Database Security Notification Law that the Plaintiff proposes to represent, in that all of Plaintiff's claims are based on the same legal theories, arise from the same actions involving the acts and omissions of 1st Lake Properties.

c. Typicality

74. Pursuant to F.R.C.P 23(a)(3), the claims of the class representatives' (i.e., Plaintiffs) are typical of the claims of the Class Members, as each arises from the same Data

Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

75. Further, 1st Lake Properties' defenses to the Plaintiff's claims are typical of their defenses to the claims of the other putative class members.

d. Adequacy of Representation

76. Pursuant to F.R.C.P 23(a)(4)), the Plaintiffs, as class representatives of the Class Members, can and will fairly and adequately protect the interests of the entire class and have retained skilled attorneys, with the necessary financial means, who are experienced in the prosecution of mass tort and class actions and who will handle this action in an expeditious and economical manner; all in the best interest of all members of the class.

e. The Proposed Class Meets F.R.C.P 23(b)

77. The prosecution of separate actions by individual members of the class would create an undue risk of inconsistent and varying decisions and could establish incompatible standards of conduct for Defendant 1st Lake herein, including but not limited to the applicable duties which were owed and/or breached to Plaintiffs and others similarly situated.

78. For these same reasons, the maintenance of separate legal actions would create an undue risk of one class member setting a legal precedent which would be dispositive of the interests of the class members who were not parties to the case then being adjudicated. Such separate actions would substantially impair or impede the absent class members' ability to protect their interests.

79. Accordingly, a class action would be fair to the individual members of the class and to Defendant 1st Lake, as numerous individual claims could result in inconsistent or

varying adjudications regarding the individual members of the class, thereby potentially damaging the rights of both the class members and the Defendants herein.

80. Further, individual litigation of the claims at issue herein would only increase the delays and expenses to all parties in the court systems for resolving the controversies and issues presented. The class action methodology provided by F.R.C.P. 23 is to facilitate the Court by providing for judicial economy, reduce management difficulties, and provide the benefit of uniform and unitary adjudication.

81. In short, a class action is superior to the alternatives, if any, for the fair and efficient adjudication of the claims and controversy alleged in this First Amended Class Action Complaint for Damages. Such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without duplication. Separate trials adjudicating the liability of the Defendants will be inefficient and will run the risk of producing inconsistent verdicts. There are no difficulties that would preclude class action treatment of this lawsuit, and no superior alternative exists for the fair and efficient adjudication of this controversy.

82. Plaintiffs re-allege and incorporate by reference the allegations set forth in each of the preceding paragraphs of this First Amended Class Action Complaint for Damages, with the same force and effect as if fully set forth herein, and assert the following causes of action:

V. CAUSES OF ACTION

COUNT 1 – GROSS NEGLIGENCE AND NEGLIGENCE
(On Behalf of Plaintiff and the Class)

83. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

84. Plaintiff and the Class entrusted their PII, which includes personal information as defined by R.S. 51:3073, to Defendant on the premise and with the understanding that Defendant would safeguard their PII, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

85. The PII and personal information provided by Plaintiff to Defendant was information that was not publicly available, and was otherwise not lawfully made available to the general public from federal, state, or local government records.

86. Pursuant to Louisiana R.S. 51:3074, *et seq.*, (hereafter "R.S. 51:3074"), Defendant owed a duty of care to Plaintiff and Class members to maintain reasonable security procedures and practices appropriate to the nature of the PII it collected to protect Plaintiff and the Class Members' personal information from unauthorized access, destruction, use, modification or disclosure.

87. It was foreseeable that Defendant's failure to maintain reasonable security procedures and practices as required by R.S. 51:3074 that were in accordance with industry standards for data security would compromise Plaintiff's and the Class's PII in a data breach. And here, that foreseeable danger came to pass.

88. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if their PII was wrongfully disclosed.

89. Defendant owed these duties to Plaintiff and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff and Class members' PII.

90. Defendant owed—to Plaintiff and Class members—at least the following duties to:

a. exercise reasonable care in handling and using the PII in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class members within a reasonable timeframe of any breach to the security of their PII.

91. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class members the scope, nature, and occurrence of the Data Breach as required by R.S. 51:3074(C) and R.S. 51:3074(D). After all, this duty is required and necessary for Plaintiff and Class members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

92. Defendant also had a duty take all reasonable steps to destroy or arrange for the destruction of records within its custody or control containing personal information that is no longer needed or being used by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means, as required by R.S. 51:3074(B).

93. Defendant knew or reasonably should have known that the failure to exercise the due care and duties delineated in R.S. 51:3074, *et seq*., in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

94. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant (as an entity that conducts business in the State of Louisiana and collects personal information) and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant.

95. Defendant's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the Federal Trade Commission ("FTC"), the unfair act or practice by a business, of failing to employ reasonable measures to protect and secure PII. Various FTC publications and orders also form the basis of Defendant's duty. Federal Courts have likewise determined that this statute creates enforceable duties that are "ascertainable as it relates to data breach cases based on the text of the statute and a body of precedent interpreting the statute and applying it to the data beach context." *In re Marriott Int'l, Inc.,* 440 F. Supp. 3d 447, 481 (D. Md. 2020*). See also In re TJX Companies Retail Sec. Breach Litig.*, 564 F.3d 489, 498-99 (1st Cir. 2009), *as amended on reh'g in part* (May 5, 2009) (applying FTC precedent for scope of duty under state law based on Section 5 of the FTC Act).

96. This duty included, among other things, designing, maintaining, and testing its security systems to ensure that Plaintiffs' and the Class's PHI and PII was adequately protected and secured. Defendant further had a duty to implement processes that would detect a breach of their security system in a timely manner.

97. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and the Class's PII and not complying with industry standards.

Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach.

98. The harm occurring as a result of the Data Breach is the type of harm that Section 5 of the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class.

99. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant hold vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII — whether by malware or otherwise.

100. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class members' and the importance of exercising reasonable care in handling it.

101. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

102. Defendant breached these duties as evidenced by the Data Breach.

103. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff and Class members' PII by:

a. disclosing and providing access to this information to third parties;

b. failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information to protect the

personal information from unauthorized access, destruction, use, modification or disclosure as required by R.S. §51:3074(A);

c. failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen;

d. failing to take reasonable steps to destroy or arrange for the destruction of the records within its custody or control that contained personal information that was no longer in use by Defendant, as required by R.S. §51:3074(B);

104. Defendant breached its duties delineated in R.S. §51:3074(A) and §51:3074(B) by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and Class members which actually and proximately caused the Data Breach and Plaintiff and Class members' injury.

105. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class members as required by R.S. §51:3074(C) and §51:3074(D), which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class members' injuries-in-fact.

106. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

107. As a direct and traceable result of Defendant's gross negligence and/or negligent supervision, Plaintiff and Class members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

108. Defendant's breach of its specific duties delineated in R.S. § 51:3074 caused Plaintiff and Class members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT TWO: VIOLATION OF LA. RS §§ 51:3071 *ET SEQ.*
Louisiana Database Security Breach Notification Law
(On Behalf of Plaintiff and the Class)

109. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

110. With the "Database Security Breach Notification Law," the Louisiana Legislature recognized the importance of data security—and the severe damage that data breaches inflict on its citizens. La. RS § 51:3071 et seq. In particular, the Louisiana Legislature declared:

a. "The crime of identity theft is on the rise in the United States. Criminals who steal personal information use the information to open credit card accounts, write bad checks, buy automobiles, and commit other financial crimes using the identity of another person." La. RS. § 51:3072(3).

b. "The privacy and financial security of individuals are increasingly at risk due to the ever more widespread collection of personal information." RS § 51:3072(1).

c. "Identity theft is costly to the marketplace and to consumers." RS § 51:3072(4).

d. "Victims of identity theft must act quickly to minimize the damage; therefore, expeditious notification of possible misuse of a person's personal information is imperative." RS § 51:3072(5).

111. Defendant's Data Breach constitutes a "breach of the security of the system" under these statutes because Defendant's Data Breach compromised the security, confidentiality, and/or integrity of Plaintiff's and Class Members' PII (computerized data) which very likely resulted in the unauthorized acquisition of that PII.

112. Defendant constitutes a "person" under these statutes because Defendant is a legal entity.

113. Plaintiff's and Class Members' exposed PII constitutes "personal information" under these statutes because their exposed PII includes computerized formats of their: names, Social Security numbers, and account numbers. Such information is not publicly available.

114. Because Defendant "conducts business in the state," RS § 51:3074(A) requires that Defendant "shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

115. Because Defendant "maintains computerized data that includes personal information that [it] does not own," RS § 51:3074(D)-(E) requires that Defendant "notify the owner . . . of the information" and "in the most expedient time possible and without unreasonable delay but not later than sixty days from the discovery of the breach." In this case, Defendant waited until two-hundred and nine days after it discovered the Data Breach to notify many of its victims.

116. In short, Defendant violated Louisiana law when it failed to disclose in a timely manner to Plaintiff and Class Members that their PII was disclosed in the Data Breach. Thus, Plaintiff and Class Members are entitled—under RS § 51:3075—to recover damages caused by Defendant's failures.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff Kevin Merrill individually and as representative of a putative class of persons similarly situated, prays that:

A. a jury trial be had on all issues; and after due proceedings be had, that this action be certified as a class action pursuant to the provisions of F.R.C.P 23, *et seq*.,

B. that judgment be entered in favor of Plaintiffs and others similarly situated against Defendant in a sum sufficient to compensate Plaintiffs and others similarly situated for the following:

   i. declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;

   ii. injunctive relief as necessary to protect the interests of Plaintiff and the

   iii. damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

   iv. restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

   v. attorneys' fees and costs, as allowed by law; and

vi. prejudgment and post-judgment interest, as provided by law.

Date: October 17, 2023

Respectfully submitted,

By: /s/ Layne C. Hilton

Layne C. Hilton (La. Bar No. 36990)
MEYER WILSON, CO., LPA
900 Camp Street, Suite 337
New Orleans, LA 70130
Telephone: 614-255-2697
lhilton@meyerwilson.com

Matthew R. Wilson
Pro Hac Vice Forthcoming
MEYER WILSON CO., LPA
305 W. Nationwide Blvd
Columbus, OH 43215
Tel. (614) 224-6000
mwilson@meyerwilson.com

TURKE & STRAUSS LLP
Samuel J. Strauss
Pro Hac Vice Forthcoming
Raina Borrelli
Pro Hac Vice Forthcoming
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
sam@turkestrauss.com
raina@turkestrauss.com

Attorneys for Plaintiff and Proposed Class