

24<sup>th</sup> JUDICIAL DISTRICT COURT FOR THE PARISH OF JEFFERSON

P1 035

STATE OF LOUISIANA

NO.: 030-959

DIVISION: "O"

KEVIN MERRELL, INDIVIDUALLY AND ON BEHALF  
ALL OTHERS SIMILARLY SITUATED,

VERSUS

1ST LAKE PROPERTIES, INC.

FILED: \_\_\_\_\_

DEPUTY CLERK

**CLASS ACTION PETITION AND DEMAND FOR JURY TRIAL**

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

**PARTIES**

1.

Made and named Petitioner herein, individually, and as a representative of a putative class of persons similarly situation, is Kevin Merrell. Petitioner is a person of the full age of majority and domiciled in the Parish of Jefferson, State of Louisiana. Petitioner 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 1<sup>st</sup> Lake Properties, and who had their PII breached due to 1<sup>st</sup> Lake's misconduct.

2.

Made and named 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. 1<sup>st</sup> Lake Properties may be served through its registered agent: William Henry Shane, Jr., 3925 N. I-10 Service Road W. #105, Metairie, Louisiana, 70002

**JURISDICTION AND VENUE**

3.

This Court has jurisdiction over this matter because the Defendant subjected themselves to the jurisdiction of the Court by conducting business in this parish and this State, and because the

amount in controversy in this matter and the subject matter upon which it is based are sufficient to justify jurisdiction in this Court pursuant to Louisiana Code of Civil Procedure Art. 2.

4.

There is no federal subject matter jurisdiction over this action because there is not complete diversity between the parties; because this action does not raise any federal questions; and because this action does not assert any federal claims or causes of action. Upon information and belief, most (if not all) putative class members are domiciled in Louisiana, and Defendant is a domestic corporation domiciled in Louisiana.

5.

Venue is proper in this Court pursuant to Louisiana Code of Civil Procedure Art. 42(2) because Defendant 1st Lake Properties is a domestic corporation domiciled in the Parish of Jefferson and maintains a registered office in the Parish of Jefferson.

6.

Venue is also proper in this Court pursuant to Louisiana Code of Civil Procedure Article 593(A) because this is an action brought on behalf of a class against a Defendant in a parish of proper venue as to that Defendant, as set forth in Louisiana Code of Civil Procedure Art. 42(2).

### **FACTUAL BACKGROUND**

#### **Defendant Collected and Stored the PII of Petitioner and the Class**

7.

Defendant is a developer and property manager in the New Orleans area.<sup>1</sup>

8.

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

9.

---

<sup>1</sup> *About 1st Lake Properties*, 1ST LAKE, <https://1stlake.com/new-orleans-apartments-1st-lake/> (last visited Mar. 16, 2023).

<sup>2</sup> *Id.*

<sup>3</sup> *Id.*

<sup>4</sup> *Id.*

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.”<sup>5</sup>

10.

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, Petitioner and Class members themselves took reasonable steps to secure their PII.

11.

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.

12.

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

13.

Defendant recognizes these duties, declaring that:

- a. “we have put in place appropriate physical, electronic and managerial procedures reasonably designed to safeguard the information we collect,”<sup>6</sup> and
- b. “[1st Lake] is committed to providing each of our users with a safe and satisfying experience;”<sup>7</sup> and
- c. “We are fully committed to protecting your personal information.”<sup>8</sup>

#### **Defendant’s Data Breach**

14.

On December 25, 2021, Defendant realized that it was hacked.<sup>9</sup> 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.<sup>10</sup>

15.

---

<sup>5</sup> *Id.*

<sup>6</sup> *Privacy Policy*, 1ST LAKE, <https://1stlake.com/privacy-policy/> (last visited Mar. 16, 2023).

<sup>7</sup> *Id.*

<sup>8</sup> *Notice*, MAINE ATTORNEY GENERAL, <https://apps.web.maine.gov/online/aeviewer/ME/40/7084c924-267d-4aa3-8483-a2b1c6e426ab.shtml> (last visited Mar. 16, 2023).

<sup>9</sup> *Id.*

<sup>10</sup> *Id.*

Defendant states that it “issued its first round of notices” to its Data Breach victims on February 18, 2022.<sup>11</sup> 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.<sup>12</sup>

16.

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.

17.

And when Defendant did notify Petitioner 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 Petitioner and the Class that:

- a. “We recommend you take precautions.”
- b. “Freeze your credit file.”
- c. “Place fraud alerts on your credit file.”
- d. “Remain vigilant: review your account statements & report fraud.”
- e. “Order your free annual credit reports.”
- f. “Change passwords and security verification questions and answers.”
- g. “Obtain information about preventing identity theft, fraud alerts, security freezes and FCRA from the Federal Trade Commission.”
- h. “Obtain information about preventing identity theft from your state attorney general.”<sup>13</sup>

18.

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

---

<sup>11</sup> *Id.*

<sup>12</sup> *Id.*

<sup>13</sup> *Id.*

f. debit card numbers.<sup>14</sup>

19.

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.

20.

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.

21.

Since the breach, Defendant advertises that “1st Lake Properties is continuing to take steps to enhance its security.”<sup>15</sup> 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.

22.

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 Petitioner and Class members for the injuries that Defendant inflicted upon them.

23.

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

### **Petitioner’s Experiences and Injuries**

24.

---

<sup>14</sup> *Data Security Breach Reports*, ATTORNEY GENERAL TEXAS, <https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage> (last visited Mar. 16, 2023).

<sup>15</sup> *Notice*, MAINE ATTORNEY GENERAL, <https://apps.web.maine.gov/online/aeviewer/ME/40/7084c924-267d-4aa3-8483-a2b1c6e426ab.shtml> (last visited Mar. 16, 2023).

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

25.

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

26.

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

27.

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

28.

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

29.

Petitioner received a Notice of Data Breach in late 2022.

30.

Through its Data Breach, Defendant compromised, upon information and belief, Petitioner'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.

31.

Defendant's negligence inflicted a number of injuries upon Petitioner.

32.

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

33.

Petitioner 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 Petitioner to file a police report for identity theft in order to have these charges removed.

34.

Additionally, Petitioner 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.

35.

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

36.

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

37.

Because of Defendant's Data Breach, Petitioner 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, Petitioner's injuries are precisely the type of injuries that the law contemplates and addresses.

38.

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

39.

Petitioner 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.

40.

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

41.

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

42.

Today, Petitioner 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.

**Petitioner and the Proposed Class Face Significant Risk of Continued Identity Theft**

43.

Because of Defendant’s failure to prevent the Data Breach, Petitioner 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 at risk for future breaches so long as Defendant fails to take appropriate measures to protect the PII.

44.

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.

45.

The value of Petitioner 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.

46.

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.

47.

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.).

48.

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

49.

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 Petitioner and Class members, and it is reasonable for any trier of fact, including this Court or

a jury, to find that Petitioner and other Class members' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

50.

Defendant disclosed the PII of Petitioner and Class members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Petitioner 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.

51.

Defendant's failure to promptly and properly notify Petitioner and Class members of the Data Breach exacerbated Petitioner 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.

**Defendant Knew—Or Should Have Known—of the Risk of a Data Breach**

52.

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

53.

In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.<sup>16</sup>

54.

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."<sup>17</sup>

55.

---

<sup>16</sup> See *2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) <https://notified.idtheftcenter.org/s/>.

<sup>17</sup> 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>.

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.

#### **Defendant Failed to Follow FTC Guidelines**

56.

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.

57.

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.<sup>18</sup> 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.

58.

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.

59.

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;
- e. monitor for suspicious activity on the network; and
- f. verify that third-party service providers use reasonable security measures.

60.

---

<sup>18</sup> *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](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf).

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.

61.

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.

#### **Defendant Failed to Follow Industry Standards**

62.

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.

63.

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.

64.

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.

65.

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.

**CLASS ACTION ALLEGATIONS**

66.

Petitioner seeks to have this matter proceed as a Class Action pursuant to Louisiana Code of Civil Procedure Art. 591, et seq., individually and on behalf of a class of individuals similarly situated, as Petitioner 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.

67.

Petitioner, 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 Petitioners 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.

68.

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.

69.

Petitioner 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.

70.

This action is properly maintainable as a class action pursuant to Louisiana Civil Code of Procedure Article 591(A) for the following reasons:

### **Numerosity**

71.

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.

72.

Accordingly, and pursuant to La. C.C.P. Art. 591(A)(1), the number of individuals sought to be made class members is so numerous that joinder of all members would be impracticable.

73.

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.

### **Commonality**

74.

Pursuant to La. C.C.P. Art. 591(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 Petitioner' 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 Petitioner 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 Petitioner and the Class injuries;

- h. what the proper damages measure is; and
- i. if Petitioner and the Class are entitled to damages, treble damages, and or injunctive relief.

75.

Petitioner's claims asserted herein are all similar in nature and typical of the claims of each potential class member that the Petitioner proposes to represent, in that all of Petitioner's claims are based on the same legal theories, arise from the same actions involving the acts and omissions of 1st Lake Properties.

#### **Typicality**

76.

Pursuant to La. C.C.P. Art. 591(A)(3), the claims of the class representatives' (i.e., Petitioners) 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.

77.

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

#### **Adequacy of Representation**

78.

Pursuant to La. C.C.P. Art. 591(A)(4), the Petitioners, 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.

#### **Objectively Defined Class**

79.

Pursuant to La. C.C.P. Art. 591(A)(5), the class is capable of definition by objectively discernable criteria or factors, which will enable the Court to determine the consistency or membership of the class for the purpose of being able to render a conclusive judgment in this case.

80.

The proposed class is sufficiently defined in order to give potential class members enough information to determine whether they are included within the class and to enable potential class members whether to opt out of the class.

81.

Additionally, this action is properly maintainable as a class action pursuant to Louisiana Civil Code of Procedure Article 591(B) for the following reasons:

82.

Pursuant to La. C.C.P. Art. 591(B), 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 D.R. Horton and/or Bell Mechanical herein, including but not limited to the applicable duties which were owed and/or breached to Petitioners and others similarly situated.

83.

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.

84.

Accordingly, a class action would be fair to the individual members of the class and to D.R. Horton and Bell Mechanical, 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.

85.

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 La. C.C.P. Art. 591 is to facilitate the Court by providing for judicial economy, reduce management difficulties, and provide the benefit of uniform and unitary adjudication.

86.

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 Class Action Petition 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.

87.

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

#### **CAUSES OF ACTION**

##### **COUNT 1 – GROSS NEGLIGENCE AND NEGLIGENCE** **(On Behalf of Petitioner and the Class)**

88.

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

89.

Petitioner and the Class entrusted their PII 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.

90.

Defendant owed a duty of care to Petitioner and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII in a data breach. And here, that foreseeable danger came to pass.

91.

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

92.

Defendant owed these duties to Petitioner 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 Petitioner and Class members' PII.

93.

Defendant owed—to Petitioner 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 Petitioner and Class members within a reasonable timeframe of any breach to the security of their PII.

94.

Thus, Defendant owed a duty to timely and accurately disclose to Petitioner and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Petitioner 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.

95.

Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain under applicable regulations.

96.

Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Petitioner and the Class involved an unreasonable risk of harm to Petitioner and the Class, even if the harm occurred through the criminal acts of a third party.

97.

Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Petitioner and the Class. That special relationship

arose because Petitioner and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant.

98.

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.

99.

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

100.

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

101.

Defendant breached these duties as evidenced by the Data Breach.

102.

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

- a. disclosing and providing access to this information to third parties and
- b. 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.

103.

Defendant breached its duties 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 Petitioner and Class members which actually and proximately caused the Data Breach and Petitioner and Class members' injury.

104.

Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Petitioner and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Petitioner and Class members' injuries-in-fact.

105.

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

106.

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

107.

Defendant's breach of its common-law duties to exercise reasonable care and its failures and gross negligence actually and proximately caused Petitioner 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 – NEGLIGENCE *PER SE***  
**(On Behalf of Petitioner and the Class)**

108.

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

109.

Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Petitioner and Class members' PII.

110.

Section 5 of the FTC Act 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 the PII entrusted to it. The FTC

publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Petitioner and the Class members' sensitive PII.

111.

Defendant breached its respective duties to Petitioner and Class members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

112.

Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

113.

The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Petitioner and members of the Class.

114.

But for Defendant's wrongful and negligent breach of its duties owed, Petitioner and Class members would not have been injured.

115.

The injury and harm suffered by Petitioner and Class members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Petitioner and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

116.

Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence per se.

117.

As a direct and proximate result of Defendant's negligence per se, Petitioner and Class members have suffered and will continue to suffer numerous injuries (as detailed supra).

**COUNT THREE - BREACH OF FIDUCIARY DUTY**  
**(On Behalf of Petitioner and the Class)**

118.

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

119.

Given the relationship between Defendant and Petitioner and Class members, where Defendant became guardian of Petitioner and Class members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Petitioner and Class members, (1) for the safeguarding of Petitioner and Class members' PII; (2) to timely notify Petitioner and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

120.

Defendant has a fiduciary duty to act for the benefit of Petitioner and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

121.

Because of the highly sensitive nature of the PII, Petitioner and Class members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

122.

Defendant breached its fiduciary duties to Petitioner and Class members by failing to sufficiently encrypt or otherwise protect Petitioner and Class members' PII.

123.

Defendant also breached its fiduciary duties to Petitioner and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

124.

As a direct and proximate result of Defendant's breach of its fiduciary duties, Petitioner and Class members have suffered and will continue to suffer numerous injuries (as detailed supra).

**COUNT FOUR - INVASION OF PRIVACY**  
**(On Behalf of Petitioner and the Class)**

125.

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

126.

Louisiana recognizes the tort of invasion of privacy.

127.

Through its Data Breach, Defendant acted unreasonably and seriously interfered with Petitioner's and Class Members' privacy interests.

128.

Petitioner and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

129.

Defendant owed a duty to its current and former tenants, including Petitioner and the Class, to keep this information confidential.

130.

The unauthorized acquisition (i.e., theft) by a third party of Petitioner and Class members' PII is highly offensive to a reasonable person.

131.

The intrusion was into a place or thing which was private and entitled to be private. Petitioner and the Class disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Petitioner and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

132.

The Data Breach constitutes an intentional interference with Petitioner and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

133.

Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

134.

Defendant acted with a knowing state of mind when it failed to notify Petitioner and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

135.

Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Petitioner and the Class.

136.

As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Petitioner and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Petitioner and the Class to suffer damages (as detailed *supra*).

137.

Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Petitioner and the Class since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

138.

Petitioner and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Petitioner and the Class.

139.

In addition to injunctive relief, Petitioner, on behalf of himself and the other Class members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

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

140.

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

141.

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).

142.

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 Petitioner’s and Class Members’ PII (computerized data) which very likely resulted in the unauthorized acquisition of that PII.

143.

Defendant constitutes a “person” under these statutes because Defendant is a legal entity.

144.

Petitioner’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.

145.

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.”

146.

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.

147.

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

#### **PRAYER FOR RELIEF**

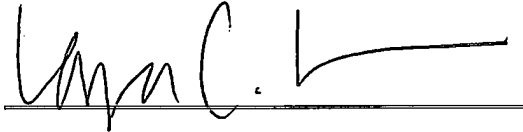
WHEREFORE, Petitioner Kevin Merrill individually and as representative of a putative class of persons similarly situated, prays that:

- A. 1<sup>st</sup> Lake Properties be served with this Class Action Petition for Damages;
- B. that said Defendant be cited to appear and answer same;
- C. that 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 La. C.C.P. art. 591 *et seq.*,
- D. that judgment be entered in favor of Petitioners and others similarly situated against Defendant in a sum sufficient to compensate Petitioners and others similarly situated for the following:
  - i. declaratory and other equitable relief as necessary to protect the interests of Petitioner and the Class;
  - ii. injunctive relief as necessary to protect the interests of Petitioner and the

- iii. damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;
- iv. restitution and damages to Petitioner 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: March 22, 2023

Respectfully submitted,

By: 

Layne C. Hilton (La. Bar No. 36990)  
**MEYER WILSON, CO., LPA**  
900 Camp Street, Suite 337  
New Orleans, LA 70130  
Telephone: 614-255-2697  
Facsimile: (614) 224-6066  
[lhilton@meyerwilson.com](mailto: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  
Fax. (614) 224-6066  
[mwilson@meyerwilson.com](mailto: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  
Facsimile: (608) 509-4423  
[sam@turkestrauss.com](mailto:sam@turkestrauss.com)  
[raina@turkestrauss.com](mailto:raina@turkestrauss.com)

*Attorneys for Petitioner and Proposed Class*

**PLEASE SERVE:**

**1<sup>st</sup> Lake Properties, Inc.**

Through its registered agent for service of process:

William Henry Shane, Jr.,

3925 N. I-10 Service Road W. #105,

Metairie, Louisiana, 70002