Daniel M. Hodes, Esq.
HODES MILMAN IKUTA, LLP
9210 Irvine Center Drive
Irvine, CA 92618
Phone: (949) 640-8222
Fax: (949) 336-8114
dhodes@hodesmilman.com

Joseph M. Lyon (*Pro Hac Vice Forthcoming*)
THE LYON FIRM, LLC
2754 Erie Avenue
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 721-1178
jlyon@thelyonfirm.com

Counsel for Plaintiffs and the Class

[Additional counsel listed on next page]

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
WESTERN DIVISION

LAUREN WATERS, an individual; JEFF HARRINGTON, an individual; and DAVID THOMPSON, an individual;
On behalf of themselves and those similarly situated,

Plaintiffs,

v.

TIMIOS, INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT FOR DAMAGES FOR:

1. **Negligence**
2. **Negligence *Per Se***
3. **Breach of Implied Contract**
4. **Unjust Enrichment**

JURY TRIAL DEMANDED

J. Scott Scheper, Esq.
STRATEGE LAW LLP
5060 N. Harbor Dr., Suite 275
San Diego, California 92106
Phone: (619) 677-5800
scheper@strategelaw.com

Terence R. Coates (*Pro Hac Vice Forthcoming*)
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com

Counsel for Plaintiffs and the Class

Plaintiffs Lauren Waters, Jeff Harrington, and David Thompson ("Plaintiffs"), individually and on behalf of all others similarly situated ("Class Members"), bring this Class Action Complaint against Timios, Inc. ("Defendant" or "Timios"), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard personally identifiable information ("PII") including name, social security number, driver's license or state issues identification number, passport number, tax identification number, military identification number, financial account number, payment card number and date of birth.

2. Timios, Inc. is a Title and Escrow Service company that provides real estate transaction services to buyers, sellers, and professionals. Timios offers their services to 44 states plus D.C. It has performed more than 380,000 transactions across their service areas.

3. As part of its services, Timios requires that its customers provide Timios with PII including name, social security number, driver's license or state issues identification number, passport number, tax identification number, military identification number, financial account number, payment card number and date of birth.

4. By obtaining, collecting, using, and deriving benefit from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties to those persons, and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure or criminal hacking activity.

5. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiffs and Class Members, to keep their PII confidential, safe, secure, and protected from unauthorized disclosure or access.

6. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

7. Plaintiffs and Class Members reasonably expected and relied upon Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

8. Defendant, however, breached its numerous duties and obligations by failing to implement and maintain reasonable safeguards; failing to comply with industry-standard data security practices and federal and state laws and regulations governing data security; failing to properly train its employees on data security measures and protocols; failing to timely recognize and detect unauthorized third parties accessing its system and that substantial amounts of data had been compromised; and failing to timely notify the impacted Class Members.

9. Timios has confirmed that between July 19-25, 2021 criminals were able to access certain devices in Timios's network (the "Data Breach"). These criminals maintained unfettered access to Defendant's network and Plaintiffs and Class Members PII for at least seven days.

10. In this day and age of regular and consistent data security attacks and data breaches, in particular in the financial industries, and given the sensitivity of the data entrusted to Timios's Data Breach is particularly egregious.

11. By implementing and maintaining reasonable safeguards and complying with standard data security practices, Defendant could have prevented this Data Breach.

12. Moreover, despite learning of the Data Breach on or about July 30, 2021, Defendant did not begin notifying customers affected by the breach until October 8, 2021.

13. Plaintiffs and members of the proposed Class have suffered actual, concrete, and imminent injuries as a direct result of Defendant's data security failures and the Data Breach. The injuries suffered by Plaintiffs and the Class Members as a direct result of the Data Breach include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiffs' and Class Members' PII; (b) economic costs associated

with the time spent to detect and prevent identity theft, including loss of productivity; (c) monetary costs associated with the detection and prevention of identity theft; (d) economic costs, including time and money, related to incidents of actual identity theft; (e) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their PII; (f) the diminution in the value of the services bargained for as Plaintiffs and Class Members were deprived of the data protection and security that Defendant promised when Plaintiffs and the proposed class entrusted Defendant with their PII; and (g) the continued and substantial risk to Plaintiffs and Class Members PII, which remains in the Defendant's possession of Defendant with in-adequate measures to protect Plaintiffs' and Class Members' PII.

14. Plaintiffs seek to remedy these harms, and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and remains at risk due to inadequate data security.

15. Accordingly, Plaintiffs, on behalf of themselves and the Class Members, assert claims for negligence, negligence per se, breach of implied contract, and unjust enrichment. Plaintiffs seek injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity or by law.

THE PARTIES

Plaintiff Lauren Waters

16. Plaintiff Lauren Waters is a natural person and resident and citizen of the State of Mississippi. Plaintiff Waters received a Notice of Data Breach from Defendant, dated October 8, 2021, stating that her information, including one or more of the following, was accessed or acquired by an unauthorized party in the Data Breach: name, social security number, driver's license or state issues identification number, passport number, tax identification number, military identification number, financial account number, payment card number and date of birth."

17. Before this Data Breach, Plaintiff Waters had taken steps to protect against keeping the information safe.

18. Plaintiff Waters has suffered actual damages and is at imminent, impending, and substantial risk for identity theft and future economic harm due to the highly sensitive nature of the information that was targeted and stolen. Since learning about the breach, in an effort to mitigate the risk, Plaintiff Waters has spent time and effort reviewing financial statements to detect and prevent identity theft. Plaintiff Waters has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the theft and compromise of his PII. She will spend additional time and incur future economic costs associated with the detection and prevention of identity theft.

Plaintiff Jeff Harrington

19. Plaintiff Jeff Harrington is a natural person and resident of the State of Pennsylvania. Plaintiff Harrington received a Notice of Data Breach from Defendant, dated October 8, 2021, stating that his information, including one or more of the following, was accessed or acquired by an unauthorized party in the Data Breach: name, social security number, driver's license or state issues identification number, passport number, tax identification number, military identification number, financial account number, payment card number and date of birth."

20. Before this Data Breach, Plaintiff Harrington had taken steps to protect against keeping the information safe.

21. Plaintiff Harrington has suffered actual damages and is at imminent, impending, and substantial risk for identity theft and future economic harm due to the highly sensitive nature of the information that was targeted and stolen. Since learning about the breach, in an effort to mitigate the risk, Plaintiff Harrington has spent time and effort reviewing financial statements to detect and prevent identity theft and calling Credit Agencies. Plaintiff Harrington has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the theft and compromise of his PII. He will spend additional time and incur future economic costs

associated with the detection and prevention of identity theft.

Plaintiff David Thompson

22. Plaintiff David Thompson is a natural person and resident of the State of Pennsylvania. Plaintiff Thompson received a Notice of Data Breach from Defendant, dated October 8, 2021, stating that his information, including one or more of the following, was accessed or acquired by an unauthorized party in the Data Breach: name, social security number, driver's license or state issues identification number, passport number, tax identification number, military identification number, financial account number, payment card number and date of birth."

23. Before this Data Breach, Plaintiff Thompson had taken steps to protect against keeping the information safe.

24. Plaintiff Thompson has suffered actual damages and is at imminent, impending, and substantial risk for identity theft and future economic harm due to the highly sensitive nature of the information that was targeted and stolen. Since learning about the breach, in an effort to mitigate the risk, Plaintiff Thompson has spent time and effort reviewing financial statements to detect and prevent identity theft and calling Credit Agencies. Plaintiff Thompson has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the theft and compromise of his PII. He will spend additional time and incur future economic costs associated with the detection and prevention of identity theft.

Defendant Timios, Inc.

25. Defendant Timios, Inc., is a Delaware corporation with its principal place of business located at 19360 Ventura Blvd. Tarzana, California, 91356. Service of Process is proper on Kevin Lam at 340 South Lemon Ave 7227, Walnut, California, 91361.

JURISDICTION & VENUE

26. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. 1332(d)(2). The matter in controversy

exceeds $5,000,000 in the aggregate, exclusive of interest and costs. Further, Plaintiffs alleges a nationwide class, and Plaintiffs, as proposed Class representatives, are citizens of different states than Defendant.

27. Venue is appropriate in this District under 28 U.S.C. § 1391(a) because Timios is based in this District, and because a substantial portion of the events giving rise to this cause of action occurred in this District.

FACTUAL ALLEGATIONS

28. Defendant "provides unparalleled real estate transaction experience for buyers, sellers, and professionals." It has had "over 380,000 transactions and $62 billion in total closings" in services in America.[1]

29. In the course of servicing real estate transactions, Defendant acquires, collects, and stores or processes a massive amount of PII, including name, social security number, driver's license or state issues identification number, passport number, tax identification number, military identification number, financial account number, payment card number and date of birth. Customers are required to provide this PII as a condition of receiving these services to process their transaction.

30. Defendant is fully aware of the sensitivity and value of the PII it stores and maintains.

31. By requiring the production of, collecting, obtaining, using, and deriving benefits from Plaintiffs' and Class Members' PII, Defendant assumed certain legal and equitable duties and knew or should have known that it was responsible for the diligent protection of the PII collected and stored.

32. Defendant's Privacy Policy (falsely) states: "We will maintain commercially reasonable technical, organizational, and physical safeguards, consistent with applicable law, to protect your personal information."[2]

---

[1] https://www.timios.com/about-us/ (last visited 10/22/2021).
[2] https://www.timios.com/privacy-policy/ (last visited 10/22/2021).

The Data Breach

33. On or about July 19-25, 2021, there was unauthorized access to certain devices in Timios's network that resulted in the encryption of some of their systems.

34. Following the unauthorized access, an investigation determined that personal information related to some individuals, including Plaintiffs, may have been accessed and/or acquired by the unauthorized actor.

35. Upon information and belief, as a result of Defendant's failure to take the necessary and required steps, and its failure to exercise reasonable care in the hiring, training, and/or supervision of its employees and agents, to secure Plaintiffs' and Class Members' PII, criminal actors were able to infiltrate and gain access to Plaintiffs and Class Members PII.

36. As a large and successful company, Defendant had the resources to invest in the necessary data security and protection measures. Yet, Defendant failed to exercise reasonable care in the hiring and/or supervision of its employees and agents and failed to undertake adequate analyses and testing of its own systems, adequate personnel training, and other data security measures to avoid the failures that resulted in the Data Breach.

37. Defendant began providing notice of the Data Breach to Plaintiffs, the Class Members, and state Attorneys General in October of 2021.

38. Defendant's notification letters acknowledge the importance of data security and Defendant's duty to Class Members, and its failures in security measures and training stating: "Timios, Inc. is committed to maintaining the integrity and the security of the data that we receive and maintain" and "are taking a number of steps to help prevent something like this from occurring again […] We implemented additional measures to further enhance our security protocols and are providing continued education and training to our employees."

The Data Breach & Associated Harms to Defendant's Customers Were Foreseeable

39. Defendant knew or should have known that it was an ideal target for hackers and those with nefarious purposes related to sensitive personal and financial data.

40. It is common knowledge that the criminal(s) that target the type of PII at issue in this case attack the systems for the purpose of using that data to commit fraud, theft, and other crimes. Criminals acquire the data for the purpose of the selling or providing the PII to other individuals on the Dark Web for the purpose to commit fraud, identity theft, and other crimes. Consequently, Plaintiffs and Class Members face a substantial risk for identity theft and the associated economic harms.

41. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers, but credit and debit cards can be cancelled, quickly mitigating the hackers' ability to cause further harm. Instead, types of PII that cannot be easily changed (such as dates of birth, Social Security Numbers, and medical history) are the most valuable to hackers.

42. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[3] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[4]

43. Identity thieves may commit various types of crimes such as, *inter alia*, immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, fraudulently obtaining medical services, and/or using the victim's information to obtain a fraudulent tax refund.

44. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected. Moreover, identify thieves may wait yearsbefore using the stolen data.

---

[3] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2012), https://www.justice.gov/usao-wdmi/file/764151/download (last visited July 28, 2021).

[4] *See id.* The FTC defines identity theft as "a fraud committed or attempted using the identifyinginformation of another person without authority." 16 CFR §603.2(a). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction withany 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, alien registration number, government passport number, employer or taxpayer identification number." 16 CFR §603.2(b).

45. The unauthorized disclosure of Social Security numbers can be particularly damaging. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns.[5] Victims of the Data Breach, including Plaintiffs, will spend, and already have spent, time contacting various agencies, such as the Internal Revenue Service and the Social Security Administration. They also now face a real and imminent substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

46. And Social Security numbers cannot easily be replaced. In order to obtain a new Social Security number a person must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, no new Social Security number can be obtained until the damage has been done.

47. Furthermore, as the Social Security Administration ("SSA") warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.

[5] When fraudulent tax returns are filed, the requirements for a legitimate taxpayer to file their tax returns with the IRS increase, including the necessity to obtain and utilize unique PIN numbers just to be able to file a tax return.

For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[6]

48. The physical, emotional, and social toll suffered (in addition to the financial toll) by identity theft victims cannot be understated.[7] "A 2016 Identity Theft Resource Center survey of identity theft victims sheds light on the prevalence of this emotional suffering caused by identitytheft: 74 percent of respondents reported feeling stressed, 69 percent reported feelings of fear related to personal financial safety, 60 percent reported anxiety, 42 percent reported fearing for thefinancial security of family members, and 8 percent reported feeling suicidal."[8]

Defendant Acknowledges the Imminent Risk of Identity Theft

49. Indeed, the notification letters received by Plaintiffs and the Class Members acknowledges the imminent risk of identity theft. Notably, Defendant has offered to provide Plaintiffs and Class Members a free one-year membership to identity protection services. Defendant would not offer to pay to provide these services absent the present, imminent and substantial risk of fraud and theft faced by Plaintiffs and the Class Members as a result of the Data Breach.

50. Similarly, the notifications sent to victims of the Data Breach warn the Plaintiffs and Class Members of the imminent risk and state: "It is best practice to remain vigilant by reviewing your account statement and credit reports for any unauthorized

---

[6] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 28, 2021).

[7] Alison Grace Johansen for NortonLifeLock, *4 Lasting Effects of Identity Theft*, (Mar. 13, 2018), https://www.lifelock.com/learn-identity-theft-resources-lasting-effects-of-identity-theft.html (last visited July 28, 2021).

[8] *Id.* (citing *Identity Theft: The Aftermath 2016™*, Identity Theft Resource Center (2016) https://www.idtheftcenter.org/images/page-docs/AftermathFinal_2016.pdf).

activity […] you should remain vigilant for incidents of fraud that may attempt to trick you into providing passwords or other information about yourself." Defendant tacitly acknowledges that Plaintiffs and Class Members may incur costs to obtain credit reports in excess of one per year. (noting the law only entitles individuals "every 12 months to one free copy of your credit report from each of the three major credit reporting companies."). Despite urging Plaintiffs and Class Members to check their credit reports, Defendant has not offered to pay costs associated with Plaintiffs and Class Members obtaining more than one free credit report each year.

51. Defendant also advised Plaintiffs and Class Members to obtain a security freeze on their credit reports. Defendant acknowledges that victims exercising their right to obtain a credit freeze will be further inconvenienced and harmed as a result of taking these reasonable steps to prevent future harm. For example, Defendant states that to implement a freeze, Plaintiffs and Class Members must take the time to "contact the three national credit reporting bureaus," and that "if you opt for a temporary lift because you are applying for credit or a job" […] you will have to "request with all three credit bureaus," or if you have find out which bureau is going to be contacted, you can request the lift from only them directly.

The PII at Issue Here is Particularly Valuable to Criminals

52. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[9]

[9] *The Information Marketplace: Merging and Exchanging Consumer Data*, FTC (Mar. 13, 2001), *transcript*

53. Consumers rightfully place a high value not only on their PII, but also on the privacy of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information – the very injury at issue here – between $11.33 and $16.58 per website. The study also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62."[10] This study was done in 2002, almost twenty years ago. The sea-change in how pervasive the Internet is in everyday lives since then indicates that these values—when associated with the loss of PII to bad actors—would be exponentially higher today.

54. Companies recognize that PII are valuable assets. Indeed, PII arevaluable commodities. A "cyber black-market" exists in which criminals openly post stolen PII on a number of Internet websites. Plaintiffs' and Class Members' compromised PII has a high value on both legitimate and black markets.

55. Some companies recognize PII as a close equivalent to personal property. Software has been created by companies to value a person's identity on the black market. The commoditization of this information is thus felt by consumers as theft of personal property in addition to an invasion of privacy.

56. Because the information Defendant allowed to be compromised and taken is of such a durable and permanent quality, the harms to Plaintiffs and the Class will continue and increase, and Plaintiffs and Class Members will continue to be at substantial risk for further imminent and future harm.

---

available at https://www.ftc.gov/news-events/events-calendar/2001/03/information-marketplace-merging-exchanging-consumer-data (last visited July 28, 2021).

[10] Il-Horn Hann, Kai-Lung Hui, *et al*, *The Value of Online Information Privacy: Evidence from the USA and Singapore*, at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), https://www.comp.nus.edu.sg /~ipng/research/ privacy.pdf (last visited July 28, 2021).

Defendant's Breached Industry Standards

57. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed for authorized purposes; encrypt information stored on computer networks, understand their networks vulnerabilities; and implement policies to correct any security problems.[11]

58. The FTC further recommends that companies not maintain PII and PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords; use industry tested methods for security; monitor for suspicious activity on the network; and verify that third party providers, such as Bricker, have implemented reasonable security measures. [12]

59. The FTC has brought enforcement actions against businesses for failing to protect customers' PII. The FTC has done this by treating a failure to employ reasonable measures to protect against unauthorized access to PII as a violation of the FTC Act, 15 U.S.C. § 45.

Defendant's Post-Breach Activity Was (and Remains) Inadequate

60. Immediate notice of a security breach is essential to protect victims such as Plaintiffs and Class Members. Defendant failed to provide such immediate notice, in fact taking more than one month to disclose to victims that there had been a breach, thus further exacerbating the harm to Plaintiffs and Class Members resulting from the Data Breach.

---

[11] Federal Trade Commission, Protecting Personal Information: A Guide for Business, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed September 24, 2021)

[12] Federal Trade Commission, Start With Security, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited September 24th, 2021)

61. There is no excuse for failing to timely notify victims of the breach.

62. Moreover, acknowledges that it has gaps in its systems and is implementing changes to enhance its data security. However, Defendant does not indicate that it will be purging or deleting Plaintiffs' data that is no longer needed for business operations. Until adequate systems are in place, and Plaintiffs and Class Members data is deleted from Defendant's systems, future data breaches that may again compromise Plaintiffs' data.

63. Plaintiffs and Class Members are now and in future at a significant risk of imminent and future fraud, misuse of their PII, and identity theft as a result of Defendant's actions and the Data Breach.

CLASS ACTION ALLEGATIONS

64. Plaintiffs bring this class action on behalf of themselves and a nationwide class defined as:

All persons who reside in the United States whose personal data was compromised as a result of the Data Breach that occurred on Defendant's systems from July 19-25, 2021 (the "Nationwide Class").

65. Where appropriate, the Nationwide Class is referred to collectively as the "Class," and members of the Nationwide Class as "Class Members."

66. Excluded from the Class are Defendant; officers, directors, and employees of Defendant; any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judges and court personnel in this case and any members of their immediate families.

67. Plaintiffs reserve the right to modify and/or amend the Nationwide Class definition, including but not limited to creating additional Subclasses, as necessary.

68. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

69. All members of the proposed Class are readily ascertainable in that Defendant has access to addresses and other contact information for all members of the Class, which can be used for providing notice to Class Members.

70. ***Numerosity***. The Nationwide Class is so numerous that joinder of all members is impracticable. Upon information and belief, the Nationwide Class includes thousands of individuals whose personal data was compromised by the Data Breach.

71. ***Commonality***. There are numerous questions of law and fact common to Plaintiffs and the Class, including the following:

- whether Defendant engaged in the wrongful conduct alleged in this Complaint;
- whether Defendant's conduct was unlawful;
- whether Defendant failed to implement and maintain reasonable systems and security procedures and practices to protect PII;
- whether Defendant failed to reasonably train and supervise its employees and agents to detect and avoid cyber attacks;
- whether Defendant unreasonable retained Plaintiffs and Class Members PII;
- whether Defendant unreasonably delayed in notifying affected customers of the Data Breach;
- whether Defendant owed a duty to Plaintiffs and members of the Class to adequately protect their personal data and to provide timely and accurate notice of the Defendant Data Breach to Plaintiffs and members of the Class;
- whether an implied contract to provide Plaintiffs and members Class adequate protection of their personal data;

- whether Defendant breached its duties to protect the personal data of Plaintiffs and members of the Class by failing to provide adequate data security and failing to provide timely and adequate notice of the Defendant Data Breach to Plaintiffs and the Class;
- whether Defendant's conduct was negligent;
- whether Defendant knew or should have known that its computer systems were vulnerable to attack;
- whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach of its systems, resulting in the loss of Class Members' personal data;
- whether Defendant wrongfully or unlawfully failed to inform Plaintiffs and members of the Class that it did not maintain computers and security practices adequate to reasonably safeguard customers' financial and personal data;
- whether Defendant should have notified the public, Plaintiffs, and Class Members immediately after it learned of the Data Breach;
- whether Plaintiffs and members of the Class suffered injury, including ascertainable losses, as a result of Defendant's conduct (or failure to act);
- whether Defendant was unjustly enriched by obtaining and retaining PII without adequate business purposes and without adequate security measures;
- whether Plaintiffs and members of the Class are entitled to recover damages; and,
- whether Plaintiffs and Class Members are entitled to declaratory relief and equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

72. ***Typicality***. Plaintiffs' claims are typical of the claims of the Class in that Plaintiffs, like all Class Members, had their personal data compromised, breached and stolen in the Data Breach. Plaintiffs and all Class Members were injured through the

uniform misconduct of Defendant described in this Complaint and assert the same claims for relief.

73. ***Adequacy***. Plaintiffs and counsel will fairly and adequately protect the interests of the Class. Plaintiffs have retained counsel who are experienced in Class action and complex litigation. Plaintiffs have no interests that are antagonistic to, or in conflict with, the interests of other members of the class.

74. ***Predominance***. The questions of law and fact common to Class Members predominate over any questions which may affect only individual members.

75. ***Superiority***. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiffs and Class Members have been harmed by Defendant's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct and/or inaction. Plaintiffs know of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action. Class certification is appropriate in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each Class member. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing Defendant to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by the members of

the Class would create risk of adjudications with respect to individual members of the Class that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

76. Class certification, therefore, is appropriate because the above common questions of law or fact predominate over any questions affecting individual members of the Class, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

77. Class certification is also appropriate because Defendant has acted and failed and refused to act in a manner that generally applies to all Class Members' PII in a manner, so final injunctive relief is appropriate with regard to the Class as a whole.

COUNT I

Negligence

(On Behalf of Plaintiffs and the Nationwide Class)

78. Plaintiffs incorporate by this reference paragraphs 1 through 77 above.

79. Plaintiffs and Class Members were required to submit non-public PII to obtain Title and Escrow services from Defendant.

80. By collecting, storing, and using Plaintiffs' and Class Members' PII, Defendant acquired and owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, securing, deleting, protecting, and safeguarding the sensitive PII, that they were required to provide to Defendant as a condition of receiving Defendant's services, from being compromised, lost, stolen, accessed and misused by unauthorized persons. Defendant was required to prevent foreseeable harm to Plaintiffs and the Class Members, and therefore had a duty to take reasonable steps to safeguard sensitive PII from unauthorized release or theft.

81. More specifically, this duty included: (1) designing, maintaining, and testing Defendant's data security systems and data storage architecture to ensure Plaintiffs' and Class Members' PII was adequately secured and protected: (2) adequately training and

supervising its employees to detect and avoid cyberattacks; (3) implementing processes that would detect an unauthorized breach of Defendant's security systems and data storage architecture in timely and adequate manner; (4) timely acting on all warnings and alerts, including public information, regarding Defendant's security vulnerabilities and potential compromise of the PII of Plaintiffs and Class Members; (5) maintaining data security measurers consistent with industry standards and applicable federal and state laws and other requirements; (6) timely and adequately informing Plaintiffs and Class Members if and when a data breach occurred to prevent foreseeable harm to them, notwithstanding undertaking (1)-(5) above; and (7) designing and implementing data storage, retention and deletion policies to destroy PII that is no longer necessary for the business purposes for which the data was provided.

82. Defendant had a common law and legal duty to prevent foreseeable harm to Plaintiffs and Class Members. The duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices in its affirmative collection and maintenance of PII from Plaintiffs and Class Members. In fact, not only was it foreseeable that Plaintiffs and Class Members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information for use in nefarious purposes, Defendant knew that it was more likely than not Plaintiffs and Class Members would be harmed as a result.

83. Defendant alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

84. There is a very close connection between Defendant's failure to follow reasonable security standards to protect its current and former users' personal data and the injury to Plaintiffs and the Class. When individuals have their personal information stolen, they are at substantial risk for imminent identity theft, and need to take steps to protect themselves, including, for example, buying credit monitoring services and purchasing or obtaining credit reports to protect themselves from identity theft.

85. If Defendant had taken reasonable security measures, data thieves would not have been able to access the personal information of Plaintiffs and the Class Members. The policy of preventing future harm weighs in favor of finding a special relationship between Defendant and Plaintiffs and the Class. If companies are not held accountable for failing to take reasonable security measures to protect their customers' personal data, they will not take the steps that are necessary to protect against future security breaches.

86. Defendant owed a duty to timely disclose the material fact that Defendant's computer systems and data security practices were inadequate to safeguard users' personal and financial data from theft.

87. Defendant breached these duties by the conduct alleged in the Complaint by, including without limitation, failing to protect its customers' personal and financial information; failing to maintain adequate computer systems and data security practices to safeguard customers' personal and financial information; failing to train its employees to detect and avoid falling victim to cyberattacks; allowing unauthorized access to Plaintiffs' and Class Members' PII; failing to disclose the material fact that Defendant's computer systems and data security practices were inadequate to safeguard customers' personal and financial data from theft; and failing to disclose in a timely and accurate manner to Plaintiffs and members of the Class the material fact of the Data Breach; and improperly retaining data that was not necessary for the business purposes for which the data was provided.

88. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their PII would not have been compromised. Specifically, as a direct and proximate result of Defendant's failure to exercise reasonable care and use commercially reasonable security measures, the personal data of Defendant's customers was accessed by ill-intentioned criminals who could and will use the information to commit identity or financial fraud. Plaintiffs and the Class Members face the imminent, certainly impending and substantially heightened risk of identity theft, fraud, and further misuse of their personal data.

89. It was foreseeable that (1) Defendant's failure to safeguard the PII of Plaintiffs and Class Members would lead to one or more types of injury to them; and (2) data breach at Defendant was foreseeable given the known high frequency of cyberattacks and data breaches in the financial industries.

90. As a direct a proximate result of Defendant's negligence, Plaintiffs and members of the proposed Class have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiffs and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiffs' and Class Members' PII; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their PII; (g) the diminution in the value of the services bargained for as Plaintiffs and Class Members were deprived of the data protection and security that Defendant promised when Plaintiffs and the proposed class entrusted Defendant with their PII; and (h) the continued and substantial risk to Plaintiffs and Class Members PII, which remains in the Defendant's possession of Defendant with in-adequate measures to protect Plaintiffs' and Class Members' PII.

COUNT II

Negligence Per Se

(On Behalf of Plaintiffs and the Nationwide Class)

91. Plaintiffs incorporate by this reference paragraphs 1 through 90 above.

92. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiffs and Class Members.

93. The FTC Act prohibits "unfair . . . practices in or affecting commerce," which the FTC has interpreted to include businesses' failure to use reasonable measures

to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

94. Pursuant to the Gramm-Leach-Bliley Act, Defendant had a duty to protect the security and confidentiality of Plaintiffs' and Class Members' PII. *See* 15 U.S.C. § 6801.

95. Pursuant to the FCRA, Defendant had a duty to adopt, implement, and maintain adequate procedures to protect the security and confidentiality of Plaintiffs' and Class Members' PII. *See* 15 U.S.C. § 1681(b).

96. Defendant solicited, gathered, and stored PII of Plaintiffs and the Class Members to facilitate transactions which affect commerce.

97. Defendant violated the FTC Act (and similar state statutes), FCRA, and the Graham-Leach-Bliley Act by failing to use reasonable measures to protect PII of Plaintiffs and Class Members and not complying with applicable industry standards, as described herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

98. Defendant's violation of the FTC Act (and similar state statutes) as well as its violations of the FCRA, and the Graham-Leach-Bliley Act constitutes negligence *per se*.

99. Plaintiffs and the Class Members are within the class of persons that the FTC Act (and similar state statutes), the FCRA, and the Graham-Leach-Bliley Act were intended to protect.

100. The harm that occurred as a result of the breach is the type of harm the FTC Act (and similar state statutes), as well as the FCRA, and the Graham-Leach-Bliley Act were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures caused the same harm as that suffered by Plaintiffs and the Class Members.

101. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered, and continue to suffer, damages arising from the breach as described herein and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

102. As a direct and proximate result of Defendant's negligence and the data breach, Plaintiffs and members of the proposed Class have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiffs and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiffs' and Class Members' PII; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their PII; (g) the diminution in the value of the services bargained for as Plaintiffs and Class Members were deprived of the data protection and security that Defendant promised when Plaintiffs and the proposed class entrusted Defendant with their PII; and (h) the continued and substantial risk to Plaintiffs and Class Members PII, which remains in the Defendant's possession of Defendant with in-adequate measures to protect Plaintiffs' and Class Members' PII.

COUNT III

Breach of Implied Contract

(On Behalf of Plaintiffs and the Nationwide Class)

103. Plaintiffs incorporate by this reference paragraphs 1 through 102 above.

104. Plaintiffs and the Class Members delivered their personal and financial information to Defendant as part of the process of obtaining services provided by Defendant.

105. Plaintiffs and members of the Class entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiffs' and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

106. In providing such data, Plaintiffs and the other members of the Class entered into an implied contract with Defendant whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiffs' and the other Class Members' sensitive, non-public information.

107. In delivering their personal data to Defendant, Plaintiffs and Class Members intended and understood that Defendant would adequately safeguard that data.

108. Plaintiffs and the Class Members would not have entrusted their private and confidential financial and personal information to Defendant in the absence of such an implied contract.

109. Defendant accepted possession of Plaintiffs' and Class Members' personal data for the purpose of providing Title and Escrow services to Plaintiffs and Class Members.

110. Had Defendant disclosed to Plaintiffs and Class Members that Defendant did not have adequate computer systems and security practices to secure users' and former users' personal data, Plaintiffs and members of the Class would not have provided their PII to Defendant.

111. Defendant recognized that its current and former customer's personal data is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and Class Members.

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

113. Defendant breached the implied contract with Plaintiffs and Class Members by failing to take reasonable measures to safeguard their data.

114. As a direct and proximate result of the breach of the contractual duties, Plaintiffs and members of the proposed Class have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiffs and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiffs' and Class Members' PII; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their PII; (g) the diminution in the value of the services bargained for as Plaintiffs and Class Members were deprived of the data protection and security that Defendant promised when Plaintiffs and the proposed class entrusted Defendant with their PII; and (h) the continued and substantial risk to Plaintiffs and Class Members PII, which remains in the Defendant's possession of Defendant with in-adequate measures to protect Plaintiffs' and Class Members' PII.

COUNT IV

Unjust Enrichment

(On Behalf of Plaintiffs and the Nationwide Class)

115. Plaintiffs incorporate by this reference paragraphs 1 through 114 above.

116. Defendant failed to provide reasonable security, safeguards, and protections to the Sensitive Information of Plaintiffs and Class Members, instead allowing an outdated system and inadequate training policies to persist which allowed the Data Breach to occur.

117. Defendant further failed to implement adequate and necessary data retention policies that unnecessarily exposed Plaintiffs and Class Members PII.

118. Defendant benefited from the retention of Plaintiffs and Class Members valuable data.

119. Defendant failed to disclose to Plaintiffs and Class Members that Defendant's business practices and data retention systems were inadequate to safeguard Plaintiffs' and the Class Members' Sensitive Information against theft, and that the PII would be retained indefinitely regardless of when the original business purpose was completed.

120. Under principles of equity and good conscience, Defendant should not be permitted to retain the money provided to Defendant for its services which belongs to Plaintiffs and Class Members because Defendant failed to provide adequate safeguards and security measures to protect Plaintiffs' and Class Members' Sensitive Information. Accordingly, Plaintiffs and the other Class Members paid for services that they did not receive.

121. Moreover, under principles of equity and good conscience, Defendant should not be permitted to retain the valuable PII that was provided to Defendant for its services which belongs to Plaintiffs and Class Members; where Defendant has no necessary business use of the data related to the services it contracted with Plaintiffs and Class Members; and where Defendant failed to provide adequate safeguards and security measures to protect Plaintiffs' and Class Members' Sensitive Information.

122. Accordingly, Plaintiffs and the other Class Members paid for services that they did not receive. And Defendant wrongfully accepted and retained these benefits (money and valuable PII) to the detriment of Plaintiffs and Class Members.

123. Defendant's enrichment at the expense of Plaintiffs and Class Members is and was unjust.

124. As a result of Defendant's wrongful conduct, as alleged above, Plaintiffs and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and

other compensation obtained by Defendant, as well as the PII provided to Defendant, plus attorneys' fees, costs, and interest thereon.

RELIEF REQUESTED

Plaintiffs, individually and on behalf of the Class, request that the Court:

1. Certify this case as a class action on behalf of the Nationwide Class defined above, appoint Plaintiffs as Class representatives, and appoint the undersigned counsel as class counsel;

2. Award declaratory, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and other Class Members;

3. Award restitution; compensatory, consequential, and general damages, including nominal damages as allowed by law in an amount to be determined at trial;

4. Award statutory damages to Plaintiffs and Class Members in an amount to be determined at trial;

5. Award Plaintiffs and Class Members their reasonable litigation expenses and attorneys' fees to the extent allowed by law;

6. Award Plaintiffs and Class Members pre- and post-judgment interest, to the extent allowable; and

7. Award such other and further relief as equity and justice may require.

/ / /

/ / /

/ / /

JURY TRIAL DEMANDED

Plaintiffs demand a jury trial on all issues so triable.

Dated: November 3, 2021

By: _____

Daniel M. Hodes, Esq.
HODES MILMAN IKUTA, LLP
9210 Irvine Center Drive
Irvine, CA 92618
Phone: (949) 842-2230
Fax: (949) 336-8114
dhodes@hodesmilman.com

Joseph M. Lyon (*Pro Hac Vice Forthcoming*)
THE LYON FIRM, LLC
2754 Erie Avenue
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 721-1178
jlyon@thelyonfirm.com

J. Scott Scheper, Esq.
STRATEGE LAW LLP
5060 N. Harbor Dr., Suite 275
San Diego, California 92106
Phone: (619) 677-5800
scheper@strategelaw.com

Terence R. Coates (*Pro Hac Vice Forthcoming*)
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com

Counsel for Plaintiffs and the Class

ClassAction.org
