M. Anderson Berry (SBN 262879)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916)777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com

Danielle L. Perry (SBN 292120)
dperry@masonllp.com
MASON LIETZ & KLINGER LLP
5101 Wisconsin Ave. NW, Ste. 305
Washington, DC 20016
Tel: 202-429-2290
Fax: 202-429-2294

Attorneys for Plaintiffs

THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

MYRON SCHELLHORN, RODNEY ALLEN, and TEDDA ALLEN, as individuals and on behalf of all others similarly situated,

Plaintiffs,

vs.

TIMIOS, INC.,

Defendant.

Case No.: 2:21-cv-08661

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs ("Plaintiffs") bring this Class Action Complaint against Timios, Inc. ("Timios" or "Defendant"), as individuals and on behalf of all others similarly situated, 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:

I. INTRODUCTION

1. Plaintiffs bring this class action against Timios to seek damages for Plaintiffs and the class of consumers who they seek to represent, as well as other equitable relief, including, without limitation, injunctive relief designed to protect the very sensitive information of Plaintiffs and other consumers. This action arises from Timios's failure to properly secure and safeguard personal identifiable information, including without limitation, unencrypted and unredacted names, Social Security numbers, driver's license or state-issued identification numbers, passport numbers, tax identification numbers, military identification numbers, financial account numbers, payment card numbers and/or date of birth (collectively, "personal identifiable information" or "PII").

2. Plaintiffs also allege Timios failed to provide timely, accurate and adequate notice to Plaintiffs and similarly situated Timios customers ("Class Members") that their PII had been lost and precisely what types of information was unencrypted and in the possession of unknown third parties.

3. On or about October 11, 2021, Timios notified state Attorneys General and many of its customers about a widespread data breach involving sensitive PII of 74,755 individuals. Timios explained that between July 19-25, 2021, Timios allowed its network to fall victim to a "unauthorized access" that culminated in "encryption of some of its systems" (which is typically a defining characteristic of a ransomware attack) beginning on or about July 25, 2021 (the "Data Breach"). Timios's investigation revealed its systems were accessed by unauthorized, unknown third-parties, exposing and allowing access to and acquisition of the PII detailed above.

4. Plaintiffs in this action were customers of Timios, and were not notified about the Data Breach until on or about October 8, 2021. Timios fails to

explain why it took the company over two months (from July 30, 2021, when Timios states its investigation determined that PII was accessed or acquired) to alert consumers that their sensitive PII had been exposed. As a result of this delayed response, Plaintiffs and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk to identity theft and various other forms of personal, social, and financial harm.

5. This unencrypted, unredacted PII was compromised due to Timios's negligent and/or careless acts and omissions and the utter failure to protect consumers' sensitive data. Hackers obtained their PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The risk to these consumers will remain for their respective lifetimes.

6. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Timios's failure to: (i) adequately protect consumers' PII; (ii) warn consumers of its inadequate information security practices; and (iii) effectively monitor Timios's network for security vulnerabilities and incidents. Timios's conduct amounts to negligence and violates federal and state statutes.

7. Plaintiffs and Class Members have suffered injury as a result of Timios's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) deprivation of rights they possess under the California Unfair Competition Law (Cal. Business & Professions Code §§ 17200, *et seq*.) (v) the continued and certainly an increased risk to their PII, which remains in Timios's possession and is subject to further unauthorized disclosures so long as Timios fails to undertake appropriate and adequate measures to protect the PII. This risk will remain for the lifetimes of Plaintiffs and Class Members.

8. Timios disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or at the very least negligently failing to take and implement adequate and reasonable measures to ensure that its customers' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

9. Plaintiff Myron Schellhorn is a Citizen of Nebraska residing in Lancaster County, Nebraska. Mr. Schellhorn received Timios's *Notice of Data Breach*, dated October 8, 2021, shortly after that date. If Mr. Schellhorn had known that Timios would not adequately protect his PII, he would not have allowed Timios access to this sensitive and private information.

10. Plaintiff Rodney Lynn Allen is a Citizen of Illinois residing in Morgan County, Illinois. Mr. Allen received Timios's *Notice of Data Breach*, dated October 8, 2021, shortly after that date. If Mr. Allen had known that Timios would not adequately protect his PII, he would not have allowed Timios access to this sensitive and private information.

11. Plaintiff Tedda Allen is a Citizen of Illinois residing in Morgan County, Illinois. Mrs. Allen received Timios's *Notice of Data Breach*, dated October 8, 2021, shortly after that date. If Mrs. Allen had known that Timios would not adequately protect her PII, she would not have allowed Timios access to this sensitive and private information.

12. Defendant Timios, Inc. is a Delaware corporation with its principal place of business at 19360 Ventura Blvd., Tarzana, CA 91356.

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

14. All of Plaintiffs' claims stated herein are asserted against Timios and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

15. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one other Class Member (including, for example, named Plaintiff Myron Schellhorn, a citizen of Nebraska) is a citizen of a state different from Defendant to establish minimal diversity.

16. The Central District of California has personal jurisdiction over Defendant named in this action because Defendant is headquartered and has its principal place of business in this District, conducts substantial business in California and this District through its headquarters, offices, and affiliates, and (upon information and belief) engaged in the conduct at issue here in this judicial district.

17. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant is headquartered and has its principal place of business in this District and has caused harm to Plaintiffs and Class Members through conduct in this District.

IV. FACTUAL ALLEGATIONS

Background

18. Timios promises that it will protect its members' privacy and remain in compliance with statutory privacy requirements. For example, Timios states in its Privacy Policy posted on its website that:

> The security of your personal information is important to us. That is why we take commercially reasonable steps to make sure your personal information is protected. We will maintain commercially reasonable technical, organizational, and physical safeguards, consistent with applicable law, to protect your personal information.[1]

19. Timios also promises consumers that "Timios does not otherwise share your personal information, except as required or permitted by law," and further promises that it "will not share your personal information with nonaffiliated third parties, except as permitted by California law."[2]

20. Plaintiffs and the Class Members, as current and former Timios customers, relied on these promises and on this sophisticated entity to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Consumers, in general, demand security to safeguard their PII, especially when Social Security numbers and other sensitive PII is involved.

21. Timios had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties.

The Data Breach

22. Beginning on or about October 8, 2021, Timios notified many of its customers and state Attorneys General about a widespread data breach involving

---

[1] Ex. 1 (Timios's Privacy Policy, also *available at*: https://www.timios.com/privacy-policy/ (last accessed October 29, 2021)

[2] *Id*.

sensitive PII of certain current and former customers.[3] Timios explained on or about July 25, 2021, it detected unauthorized access to certain devices in its network that encrypted some of its systems.

23. Through an investigation, Timios determined that the unauthorized individual or individuals had access to its systems between July 19, 2021 and July 22, 2021 (i.e. unauthorized access over six (6) calendar days).[4] This exposed over 75,000 consumers' PII to criminals.[5]

24. On July 30, 2021, an investigation commissioned by Timios determined that there was unauthorized activity on Timios's network that resulted in unauthorized third-party access to and acquisition of confidential information of Timios customers.

25. The confidential information that was accessed without authorization included names along with data elements including a "Social Security number, driver's license or state-issued identification number, passport number, tax identification number, military identification number, financial account number, payment card number and/or date of birth."[6]

26. On information and belief, the PII was not encrypted prior to the data breach.

27. Upon information and belief, the cyberattack was targeted at Timios due to its status as a major real estate, title, and escrow company that collects valuable personal, and financial data on its many customers, as well as its employees.

---

[3] Ex. 2 (Timios's *Notice of Data Breach*, dated October 11, 2021, posted by the Maine Attorney General, available at: https://apps.web.maine.gov/online/aeviewer/ME/40/3d523f04-a7f2-46c4-8653-51be860067b5.shtml (last accessed October 29, 2021)

[4] *Id.*

[5] *Id.*

[6] *Id.*

28. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII of Plaintiffs and the Class Members.

29. On or about October 8, 2021, Timios sent consumers (including Plaintiffs Schellhorn, Mr. Allen, and Mrs. Allen) a *Notice of Data Breach*, informing the recipients of the notice that their confidential data was involved, and stating:

> We [Timios] are also 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. . . .
>
> As a precaution, we are offering a complimentary one-year membership to Experian's IdentityWorks Credit 3B. This product helps detect possible misuse of your personal credit information and provides you with identity protection services focused on the identification and resolution of identity theft. . . .
>
> It is a best practice to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. As always, you should remain vigilant for incidents of fraud that may attempt to trick you into providing passwords or other information about yourself. We also encourage you to enroll in Experian IdentityWorks.[7]

30. Timios admitted in the *Notice of Data Breach* and the letters to the Attorneys General that their systems were subjected to unauthorized access beginning on or about July 19, 2021, and there is no indication that the exfiltrated

[7] *Id.*

PII was retrieved from the cybercriminals who took it.

31. The offer of credit and identity monitoring services, Timios's suggestion to "remain vigilant, as well as the express warning to be aware of "incidents of fraud that may attempt to trick you into providing passwords or other information about yourself" (such as unsolicited emails, spam phone calls, and other forms of fraud known as "social engineering") is an acknowledgment by Timios that the impacted customers are subject to an imminent threat of identity theft and financial fraud.

32. In response to the Data Breach, Timios claims, "we implemented additional measures to further enhance our security protocols and are providing continued education and training to our employees."[8] Timios admits enhanced "security protocols" were required, but there is no indication whether these steps are adequate to protect Plaintiffs' and Class Members' PII going forward.

33. Timios had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep their PII confidential and to protect it from unauthorized access and disclosure.

34. Plaintiffs and Class Members provided their PII to Timios with the reasonable expectation and mutual understanding that Timios would comply with its obligations and representations to keep such information confidential and secure from unauthorized access.

35. Timios failed to uphold its obligations to Plaintiffs and Members of the Class. As a result, Plaintiffs and Class Members have been significantly harmed and will be at a high risk of identity theft and financial fraud for many years to come.

36. Timios did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining, causing Plaintiffs' and Class Members' PII to be exposed.

[8] *Id.*

Securing PII and Preventing Breaches

37. Timios could have prevented this Data Breach by properly encrypting or otherwise protecting their equipment and computer files containing PII.

38. Timios has acknowledged the sensitive and confidential nature of the PII. To be sure, collection, maintaining, and protecting PII is vital to many of Timios's business purposes. Timios has acknowledged through conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure.

The Ransomware Attack and Data Breach were Foreseeable Risks of which Defendant was on Notice

39. It is well known that PII, including social security numbers and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

40. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[9]

41. Of the 1,473 recorded data breaches, 108 of them were in the banking/credit/financial industry, with the number of sensitive records being exposed exceeding 100 million. In fact, over 62% of the 164 million sensitive records exposed in data breaches in 2019 were exposed in those 108 breaches in the banking/credit/financial sector.[10]

---

[9] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed November 2, 2021)

[10] *Id*.

42. The 108 reported financial sector data breaches reported in 2019 exposed 100,621,770 sensitive records, compared to 2018 in which only 1,778,658 sensitive records were exposed in financial sector breaches.[11]

43. Consumers place a high value not only on their PII, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

44. Consumers are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers." There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of social security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."

45. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Timios knew or should have known that its electronic records would be targeted by cybercriminals.

46. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

47. Despite the prevalence of public announcements of data breach and

[11] *Id* at p15.

data security compromises, and despite its own acknowledgments of data security compromises, and despite their own acknowledgment of its duties to keep PII private and secure, Timios failed to take appropriate steps to protect the PII of Plaintiffs and the proposed Class from being compromised.

At All Relevant Times Timios Had a Duty to Plaintiff and Class Members to Properly Secure their Private Information

48. At all relevant times, Timios had a duty to Plaintiffs and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiffs and Class Members, and to promptly notify Plaintiffs and Class Members when Timios became aware that their PII may have been compromised.

49. Timios's duty to use reasonable security measures arose as a result of the special relationship that existed between Timios, on the one hand, and Plaintiffs and the Class Members, on the other hand. The special relationship arose because Plaintiffs and the Members of the Class entrusted Timios with their PII when they purchased financial products or services from Timios.

50. Timios had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Timios breached its common law, statutory, and other duties owed to Plaintiffs and Class Members.

51. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

52. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[12] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[13]

53. The ramifications of Timios's failure to keep its consumers' PII secure are long lasting and severe. Once PII is stolen, particularly Social Security and driver's license numbers, fraudulent use of that information and damage to victims may continue for years.

The Value of Personal Identifiable Information

54. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50

[12] 17 C.F.R. § 248.201 (2013).

[13] *Id.*

to $200.[14] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[15]

Criminals can also purchase access to entire company data breaches from $900 to $4,500.[16]

55. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your

---

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

[15] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, *available at*: https://www.privacyaffairs.com/dark-web-price-index-2021/

[16] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

identity can cause a lot of problems.[17]

56. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

57. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[18]

58. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[19]

59. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go

---

[17] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf.

[18] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[19] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[20]

60. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you.
>
> Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.[21]

[20] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last accessed November 2, 2021)

[21] Sue Poremba, *What Should I Do If My Driver's License Number is Stolen?"* (October 24, 2018) https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last accessed November 2, 2021)

61. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[22] However, this is not the case. As cybersecurity experts point out:

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks."[23]

62. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[24]

63. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[25]

64. Given the nature of the Data Breach, it is foreseeable that the compromised PII can be used by hackers and cybercriminals in a variety of

---

[22] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last accessed November 2, 2021)

[23] *Id.*

[24] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021 https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last accessed November 2, 2021)

[25] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

devastating ways. Indeed, the cybercriminals who possess Class Members' PII can easily obtain Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

65. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts.[26] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

66. To date, Timios has offered its consumers only one year of identity monitoring service. The offered services are inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

67. The injuries to Plaintiffs and Class Members were directly and proximately caused by Timios's failure to implement or maintain adequate data security measures for its current and former customers.

Timios Failed to Comply with FTC Guidelines

68. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of

[26] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, *available at*: https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[27]

69. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[28] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

70. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[29]

71. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain

---

[27] Federal Trade Commission, *Start With Security, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

[28] Federal Trade Commission, *Protecting Personal Information: A Guide for Business, available at*: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

[29] FTC, *Start With Security*, *supra* note 18.

computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

72. The FTC has brought enforcement actions against businesses for failing to protect consumer and consumer data adequately and reasonably, treating

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

73. Because Class Members entrusted Timios with their PII, Timios had, and has, a duty to the Class Members to keep their PII secure.

74. Plaintiffs and the other Class Members reasonably expected that when they provide PII to Timios, Timios would safeguard their PII.

75. Timios was at all times fully aware of its obligation to protect the personal and financial data of consumers, including Plaintiffs and members of the Classes. Timios was also aware of the significant repercussions if it failed to do so.

76. Timios's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiffs' and Class Members' Social Security numbers, driver's license numbers, financial/payment card information, and other highly sensitive and confidential information— constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Plaintiffs and Class Members Have Suffered Concrete Injury As A Result Of Defendant's Inadequate Security And The Data Breach It Allowed.

77. Plaintiffs and Class Members reasonably expected that Defendant would provide adequate security protections for their PII, and Class Members provided Defendant with sensitive personal information, including their Social Security numbers and driver's license numbers.

78. Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendant for its service, Plaintiffs and other reasonable consumers understood and expected that they were

paying for services and data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected. As such, Plaintiffs and the Class Members suffered pecuniary injury.

79. Cybercriminals capture PII to exploit it; the Class Members are now, and for the rest of their lives will be, at a heightened risk of identity theft. Plaintiffs have also incurred (and will continue to incur) damages in the form of, *inter alia*, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

80. The cybercriminals who obtained the Class Members' PII may exploit the information they obtained by selling the data in so-called "dark markets." Having obtained these names, addresses, Social Security numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money;
- filing false tax returns;
- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

81. In addition, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

82. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiffs and the other Class Members have been deprived of the value of their PII, for which there is a well-

established national and international market.

83. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.[30]

84. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[31] Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[32] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[33] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

85. As a result of the Data Breach, Plaintiffs and Class Members have already suffered damages.

86. Since the Data Breath, Defendant has represented to the Class Members that it "was unable to determine whether the unauthorized actor actually

---

[30] *Id.*

[31] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (February 23, 2012), http://www.iii.org/insuranceindustryblog/?p=267.

[32] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php.

[33] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH-IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, (*available at* https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf).

viewed any of the information," yet it is likely that the cybercriminals did steal data and did so undetected. EmiSoft, an award-winning malware-protection software company, states that "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence, especially during the preliminary stages of the investigation."[34]

87. In this case, according to Defendant's, cybercriminals had access to Class Members' data on at least July 19, 2021 to July 25, 2021.

88. Accordingly, that Defendant has not found evidence of data being viewed is not an assurance that the data were not accessed, acquired, and stolen. Indeed, the likelihood that cybercriminals stole the data covertly is significant, likely, and concerning.

Plaintiff Schellhorn's Experience

89. In or about early 2021, Plaintiff Myron Schellhorn was a Timios customer in Nebraska. He was required to supply Timios with his personal identifiable information, including but not limited to his name, address, date of birth, Social Security number, driver's license number, telephone number and email address, to participate in Timios's services.

90. Mr. Schellhorn received the *Notice of Data Breach*, dated October 8, 2021, on or about that date.

91. Mr. Schellhorn has experienced an increase in the number of phishing texts he receives on his cellphone since in or about August 2021.

92. As a result of the Data Breach notice, Mr. Schellhorn spent over eight hours dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Data Breach*, communicating with Timios representatives, communicating with his bank, exploring credit monitoring and

[34] EmiSoft Malware Lab, *The chance of data being stolen in a ransomware attack is greater than one in ten* (EMISOFT BLOG July 13, 2020), https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/.

identity theft insurance options, signing up for the credit monitoring supplied by Timios, reporting the breach to the IRS and FTC, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

93. Mr. Schellhorn is very careful about sharing PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

94. Mr. Schellhorn stores any and all documents containing PII in a safe and secure location, and shreds any documents he receives in the mail that contain any PII, or that may contain any information that could otherwise be used to compromise his credit card accounts and identity. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

95. Mr. Schellhorn suffered actual injury and damages in paying money to Timios for services before the Data Breach; expenditures which he would not have made had Timios disclosed that it lacked data security practices adequate to safeguard PII.

96. Mr. Schellhorn suffered actual injury in the form of damages and diminution in the value of his PII—a form of intangible property that he entrusted to Timios for the purpose of providing him services, which was compromised in and as a result of the Data Breach.

97. Mr. Schellhorn suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number.

98. Mr. Schellhorn has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third-parties and possibly criminals.

99. Mr. Schellhorn has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Timios's possession, is

protected and safeguarded from future breaches.

Plaintiff Rodney Lynn Allen's Experience

100. On or about July 2021, Plaintiff Rodney Lynn Allen was a Timios customer in Illinois. He was required to supply Timios with his personal identifiable information, including but not limited to his name, address, date of birth, Social Security number, driver's license number, telephone number and email address, to participate in Timios's services.

101. Mr. Allen received the *Notice of Data Breach*, dated October 8, 2021, on or about that date.

102. Mr. Allen has experienced an increase in the number of phishing texts and telephone calls he receives on his cellphone since in or about August 2021.

103. As a result of the Data Breach notice, Mr. Allen spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Data Breach*, exploring credit monitoring and identity theft insurance options, signing up for the credit monitoring supplied by Timios, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

104. Mr. Allen is very careful about sharing PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

105. Mr. Allen stores any and all documents containing PII in a safe and secure location, and shreds any documents he receives in the mail that contain any PII, or that may contain any information that could otherwise be used to compromise his credit card accounts and identity. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

106. Mr. Allen suffered actual injury and damages in paying money to Timios for services before the Data Breach; expenditures which he would not have made had Timios disclosed that it lacked data security practices adequate to safeguard PII.

107. Mr. Allen suffered actual injury in the form of damages and diminution in the value of his PII—a form of intangible property that he entrusted to Timios for the purpose of providing him services, which was compromised in and as a result of the Data Breach.

108. Mr. Allen suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number.

109. Mr. Allen has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third-parties and possibly criminals.

110. Mr. Allen has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Timios's possession, is protected and safeguarded from future breaches.

Plaintiff Tedda Allen's Experience

111. On or about July 2021, Plaintiff Tedda Allen was a Timios customer in Illinois. She was required to supply Timios with her personal identifiable information, including but not limited to her name, address, date of birth, Social Security number, driver's license number, telephone number and email address, to participate in Timios's services.

112. Mrs. Allen received the *Notice of Data Breach*, dated October 8, 2021, on or about that date.

113. Mrs. Allen has experienced an increase in the number of phishing texts and telephone calls she receives on his cellphone since in or about August 2021.

114. As a result of the Data Breach notice, Mrs. Allen spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Data Breach*, exploring credit monitoring and identity theft insurance options, signing up for the credit monitoring supplied by Timios,

and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

115. Mrs. Allen is very careful about sharing PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

116. Mrs. Allen stores any and all documents containing PII in a safe and secure location, and shreds any documents he receives in the mail that contain any PII, or that may contain any information that could otherwise be used to compromise his credit card accounts and identity. Moreover, she diligently chooses unique usernames and passwords for his various online accounts.

117. Mrs. Allen suffered actual injury and damages in paying money to Timios for services before the Data Breach; expenditures which she would not have made had Timios disclosed that it lacked data security practices adequate to safeguard PII.

118. Mrs. Allen suffered actual injury in the form of damages and diminution in the value of her PII—a form of intangible property that she entrusted to Timios for the purpose of providing her services, which was compromised in and as a result of the Data Breach.

119. Mrs. Allen suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy, especially her Social Security number.

120. Mrs. Allen has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen PII, especially her Social Security number, being placed in the hands of unauthorized third-parties and possibly criminals.

121. Mrs. Allen has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Timios's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

122. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

123. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All persons residing in the United States whose PII was compromised in the data breach first announced by Timios on or about October 8, 2021 (the "Nationwide Class").

124. The Nebraska Subclass is defined as follows:

> All persons residing in Nebraska whose PII was compromised in the data breach first announced by Timios on or about October 8, 2021 (the "Nebraska Subclass").

125. The Illinois Subclass is defined as follows:

> All persons residing in Illinois whose PII was compromised in the data breach first announced by Timios on or about October 8, 2021 (the "Illinois Subclass").

126. The above class and subclasses are herein referred to as the "Classes."

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

128. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

129. Numerosity, Fed R. Civ. P. 23(a)(1): Classes are so numerous that joinder of all members is impracticable. Timios has identified over 75,000 consumers whose PII may have been improperly accessed in the Data Breach, and the Classes are apparently identifiable within Timios's records.

130. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Timios had a duty to protect the PII of Plaintiffs and Class Members;
b. Whether Timios had respective duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;
c. Whether Timios had respective duties not to use the PII of Plaintiffs and Class Members for non-business purposes;
d. Whether Timios failed to adequately safeguard the PII of Plaintiffs and Class Members;
e. Whether and when Timios actually learned of the Data Breach;
f. Whether Timios adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;
g. Whether Timios violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;
h. Whether Timios failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
i. Whether Timios adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
j. Whether Timios engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;
k. Whether Plaintiffs and Class Members are entitled to actual, damages,

statutory damages, and/or punitive damages as a result of Timios's wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Timios's wrongful conduct;

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach;

131. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Timios's misfeasance.

132. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Timios has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. Timios's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Timios's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

133. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex consumer class action litigation, and Plaintiffs intend to prosecute this action vigorously.

134. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims

involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Timios. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

135. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Timios would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

136. The litigation of the claims brought herein is manageable. Timios's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

137. Adequate notice can be given to Class Members directly using information maintained in Timios's records.

138. Unless a Class-wide injunction is issued, Timios may continue in its failure to properly secure the PII of Class Members, Timios may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Timios may continue to act unlawfully as set forth in this Complaint.

139. Further, Timios has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

140. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Timios owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Timios breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Timios failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Timios on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Timios breached the implied contract;

f. Whether Timios adequately, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Timios failed to implement and maintain reasonable

security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Timios engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members; and,

i. Whether Class Members are entitled to actual damages, statutory damages, injunctive relief, and/or punitive damages as a result of Timios's wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class, or in the alternative, on behalf of the Subclasses)

141. Plaintiffs restate and reallege all of the foregoing Paragraphs 1 through 140 as if fully set forth herein.

142. As a condition of their using the services of Timios, consumers were obligated to provide Timios with certain PII, including their name, date of birth, address, Social Security number, driver's license, telephone number, email address, state-issued identification numbers, passport numbers, tax identification numbers, military identification numbers, financial account numbers, and payment card numbers.

143. Plaintiffs and Class Members entrusted their PII to Timios on the premise and with the understanding that Timios would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

144. Timios has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

145. Timios knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of their consumers' PII

involved an unreasonable risk of harm to Plaintiffs and Class Members, even if the harm occurred through the criminal acts of a third party.

146. Timios had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Timios's security protocols to ensure that Plaintiffs' and Class Members' information in Timios's possession was adequately secured and protected.

147. Timios also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and Class Members' PII.

148. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class Members was reasonably foreseeable, particularly in light of Timios's inadequate security practices and previous breach incidents involving Timios consumers' PII on stolen equipment.

149. Plaintiffs and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Timios knew of should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Timios's systems.

150. Timios's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Timios's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Timios's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiffs' and Class Members' PII, including basic encryption techniques freely available to Timios.

151. Plaintiffs and the Class Members had no ability to protect their PII that was in, and possibly remains in, Timios's possession.

152. Timios was in a position to protect against the harm suffered by

Plaintiffs and Class Members as a result of the Data Breach.

153. Timios had and continues to have a duty to adequately disclose that the PII of Plaintiffs and Class Members within Timios's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

154. Timios had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and Class Members.

155. Timios has admitted that the PII of Plaintiffs and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

156. Timios, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and Class Members during the time the PII was within Timios's possession or control.

157. 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.

158. These foregoing frameworks are existing and applicable industry standards in the financial services industry, and Defendant failed to comply with these accepted standards thereby opening the door to the cyber incident and causing the data breach.

159. Timios improperly and inadequately safeguarded the PII of Plaintiffs

and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

160. Timios failed to heed industry warnings and alerts to provide adequate safeguards to protect consumers' PII in the face of increased risk of theft.

161. Timios, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its consumers' PII.

162. Timios, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and Class Members the existence and scope of the Data Breach.

163. But for Timios's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the PII of Plaintiffs and Class Members would not have been compromised.

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

165. Additionally, 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 Timios, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Timios's duty in this regard.

166. Timios violated 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. Timios's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable

consequences of the immense damages that would result to Plaintiffs and Class Members.

167. Timios's violation of Section 5 of the FTC Act constitutes negligence *per se*.

168. Plaintiffs and Class members are within the class of persons that the FTC Act was intended to protect.

169. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was 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 and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

170. As a direct and proximate result of Timios's negligence and negligence *per se*, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Timios's possession and is subject to further unauthorized disclosures so long as Timios fails to undertake appropriate and adequate measures to protect the PII of consumers in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Timios's

goods and services they received.

171. As a direct and proximate result of Timios's negligence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

172. Additionally, as a direct and proximate result of Timios's negligence and negligence *per se*, Plaintiffs and Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in Timios's possession and is subject to further unauthorized disclosures so long as Timios fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT II
Breach of Confidence
(On Behalf of Plaintiffs and the Nationwide Class, or in the alternative, on behalf of the Subclasses)

173. Plaintiffs restate and reallege the foregoing Paragraphs 1 through 140 as if fully set forth herein.

174. At all times during Plaintiffs' and Class Members' interactions with Timios, Timios was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' PII that Plaintiffs and Class Members provided to Timios.

175. As alleged herein and above, Timios's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

176. Plaintiffs and Class Members provided their respective PII to Timios with the explicit and implicit understandings that Timios would protect and not permit the PII to be disseminated to any unauthorized third parties.

177. Plaintiffs and Class Members also provided their respective PII to Defendant with the explicit and implicit understandings that Timios would take precautions to protect that PII from unauthorized disclosure.

178. Timios voluntarily received in confidence Plaintiffs' and Class Members' PII with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

179. Due to Timios's failure to prevent and avoid the Data Breach from occurring, Plaintiffs' and Class Members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

180. As a direct and proximate cause of Timios's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

181. But for Timios's disclosure of Plaintiffs' and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Timios's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' PII, as well as the resulting damages.

182. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Timios's unauthorized disclosure of Plaintiffs' and Class Members' PII. Timios knew or should have known its methods of accepting and securing Plaintiffs' and Class Members' PII was inadequate as it relates to, at the very least, disposal of servers and other equipment containing Plaintiffs' and Class Members' PII.

183. As a direct and proximate result of Timios's breach of its confidence with Plaintiffs and Class Members, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention,

detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of consumers and former consumers in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Timios's goods and services they received.

184. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class, or in the alternative, on behalf of the Subclasses)

185. Plaintiffs restate and reallege the foregoing Paragraphs 1 through 140 as if fully set forth herein.

186. As a condition of receiving services, Defendant required Plaintiffs and Class Members to provide their PII, including names, Social Security numbers, driver's license numbers, addresses, dates of birth, email addresses, state-issued

identification numbers, passport numbers, tax identification numbers, military identification numbers, financial account numbers, and payment card numbers.

187. Defendant solicited and invited Plaintiffs and Class Members to provide their Private Information as part of Defendant's regular business practices.

188. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant. Defendant accepted the PII, and there was a meeting of the minds that Defendant would secure, protect, and keep the PII confidential.

189. Plaintiffs fully performed their obligations under the implied contracts with Defendant.

190. Plaintiffs would not have entered into transactions with Timios if Plaintiffs had known Timios would not protect their PII.

191. When Timios required and accepted the PII from Plaintiffs and the Class, it implied its assent to protect the information sufficiently.

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

193. Plaintiffs and Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

194. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity

theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

195. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

196. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT IV
Intrusion into Private Affairs / Invasion of Privacy
(On Behalf of Plaintiffs and All Class Members)

197. Plaintiffs restate and reallege the foregoing Paragraphs 1 through 140 as if fully set forth herein.

198. California established the right to privacy in Article I, Section 1 of the California Constitution.

199. The State of California recognizes the tort of Intrusion into Private Affairs, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977).

200. Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

201. Timios invaded Plaintiffs' and the Class Members' right to privacy by allowing the unauthorized access to Plaintiffs' and Class Members' PII and by negligently maintaining the confidentiality of Plaintiffs' and Class Members' PII, as set forth above.

202. The intrusion was offensive and objectionable to Plaintiffs, the Class Members, and to a reasonable person of ordinary sensibilities in that Plaintiffs' and Class Members' PII was disclosed without prior written authorization of Plaintiffs and the Class.

203. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiffs and the Class Members provided and disclosed their PII to Timios privately with an intention that the PII would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class Members were reasonable to believe that such information would be kept private and would not be disclosed without their written authorization.

204. As a direct and proximate result of Timios's above acts, Plaintiffs' and the Class Members' PII was viewed, distributed, and used by persons without prior written authorization and Plaintiffs and the Class Members suffered damages as described herein.

205. Timios has committed oppression, fraud, or malice by permitting the unauthorized disclosure of Plaintiffs' and the Class Members' PII with a willful and conscious disregard of Plaintiffs' and the Class Members' right to privacy.

206. Unless and until enjoined, and restrained by order of this Court, Timios's wrongful conduct will continue to cause Plaintiffs and the Class Members great and irreparable injury in that the PII maintained by Timios can be viewed, printed, distributed, and used by unauthorized persons. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiffs and the Class,

and Timios may freely treat Plaintiffs' and Class Members' PII with sub-standard and insufficient protections.

207. In failing to protect Plaintiffs and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private. Plaintiffs, therefore, seek an award of damages on behalf of themselves and the Class.

COUNT V
VIOLATION OF THE ILLINOIS CONSUMER FRAUD ACT
815 ILL. COMP. STAT. §§ 505/1, et seq.
(On Behalf of Plaintiffs Allen and Allen and the Illinois Subclass)

208. Plaintiffs restate and reallege the foregoing Paragraphs 1 through 140 as if fully set forth herein.

209. Plaintiffs Allen and Allen and the Illinois Subclass are "consumers" as that term is defined in 815 ILL. COMP. STAT. § 505/1(e).

210. Plaintiffs Allen and Allen, the Illinois Subclass and Defendant Timios are "persons" as that term is defined in 815 ILL. COMP. STAT. § 505/1(c).

211. Defendant is engaged in "trade" or "commerce," including provision of services, as those terms are defined under 815 ILL. COMP. STAT. § 505/1(f).

212. Defendant engages in the "sale" of "merchandise" (including services) as defined by 815 ILL. COMP. STAT. § 505/1(b) and (d).

213. Defendant's acts, practices and omissions were done in the course of Defendant's business of marketing, offering for sale, and selling financial services in the State of Illinois.

214. Timios engaged in deceptive and unfair acts and practices, misrepresentation and the concealment, suppression and omission of material facts

in connection with the sale and advertisement of "merchandise" (as defined in the Illinois CFA) in violation of the Illinois CFA, including, but not limited to, the following:

a. failure to maintain adequate computer systems and data security practices to safeguard current and former customers' PII;

b. failure to disclose the material fact that its computer systems and data security practices were inadequate to safeguard the personal information it was collecting and maintaining from theft;

c. failure to disclose in a timely and accurate manner to Plaintiff and the Illinois Subclass Members the material fact of Defendant's data breach;

d. misrepresenting material facts to Plaintiffs Allen and Allen and the Illinois Subclass, in connection with the sale of goods and services, by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Illinois Subclass members' PII from unauthorized disclosure, release, data breaches, and theft;

e. misrepresenting material facts to the class, in connection with sale of goods and services, by representing that Timios did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiffs' and Illinois Subclass members' PII; and

f. failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs' and Illinois Subclass members' PII from further unauthorized disclosure, release, data breaches and theft.

215. In addition, Timios failed to disclose that its computer systems were not well-protected and that Plaintiffs' and Illinois Subclass members' sensitive

information was vulnerable and susceptible to intrusion and cyberattacks constitutes deceptive and/or unfair acts or practices because Timios knew such facts would (a) be unknown to and not easily discoverable by Plaintiffs Allen and Allen and the Illinois Subclass; and (b) defeat Plaintiffs' and Illinois Subclass members' ordinary, foreseeable and reasonable expectations concerning the security of their PII on Timios's servers.

216. Timios intended that Plaintiffs Allen and Allen and the Illinois Subclass rely on its deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts, in connection with Timios's offering of goods and services and storing Plaintiffs' and Illinois Subclass members' PII on its servers, in violation of the Illinois CFA.

217. Timios also engaged in unfair acts and practices by failing to maintain the privacy and security of Plaintiffs' and Illinois Subclass members' personal information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach.

218. These unfair acts and practices violated duties imposed by laws including Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45) and similar state laws.

219. Timios's wrongful practices occurred in the course of trade or commerce.

220. Timios's wrongful practices were and are injurious to the public interest because those practices were part of a generalized course of conduct on the part of Timios that applied to all Illinois Subclass members and were repeated continuously before and after Timios obtained PII from Plaintiffs Allen and Allen and Illinois Subclass members.

221. All Illinois Subclass members (including Plaintiffs Allen and Allen) have been adversely affected by Timios's conduct and the public was and is at risk as a result thereof.

222. Timios also violated 815 ILCS 505/2 by failing to immediately notify affected customers of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, et seq., which provides, at Section 10:

> Notice of Breach.
>
> Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system.

223. 815 ILCS 530/20 provides that a violation of 815 ILCS 530/10 "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act."

224. As a result of Timios's wrongful conduct, Plaintiffs Allen and Allen and Illinois Subclass members were injured in that they never would have allowed their PII—the value of which Plaintiffs and Illinois Subclass members no long have control—to be provided to Timios if they had been told or knew that Timios failed to maintain sufficient security to keep such data from being hacked and taken by others.

225. Timios's unfair and/or deceptive conduct proximately caused Plaintiffs' and Illinois Subclass members' injuries because, had Timios maintained customer PII with adequate security, Plaintiffs Allen and Allen and the Illinois Subclass members would not have lost it.

226. As a direct and proximate result of Timios's conduct, Plaintiffs Allen and Allen and Illinois Subclass members have suffered harm, including, but not limited to, loss of time and money resolving fraud and fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchase of education services from Timios that Plaintiffs and Illinois

Subclass members would have never made had they known of Timios's careless approach to cybersecurity; lost control over the value of personal information; unreimbursed losses relating to fraud and fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of PII, entitling them to damages in an amount to be proven at trial.

227. Pursuant to 815 ILL. COMP. STAT. § 505/10a(a), Plaintiffs Allen and Allen seek actual, compensatory and punitive damages (pursuant to 815 ILL. COMP. STAT. § 505/10a(c)), injunctive relief, and court costs and attorneys' fees as a result of Timios's violations of the Illinois CFA.

COUNT VI
VIOLATIONS OF ILLINOIS' PERSONAL INFORMATION PROTECTION ACT
815 ILCS 530, *et seq*.
(On Behalf of Plaintiffs Allen And Allen and Illinois Subclass Members)

228. Plaintiffs restate and reallege the foregoing Paragraphs 1 through 140 as if fully set forth herein.

229. Plaintiffs Allen and Allen bring this claim on behalf of themselves and the Illinois Subclass.

230. 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.

231. Section 45 of the Illinois's Personal Information Protection Act requires entities who maintain or store "personal information concerning an Illinois resident" to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure."

232. Defendant's conduct violated the Personal Information Protection Act.

233. Specifically, Defendant voluntarily undertook the act of maintaining and storing Plaintiffs' PII but Defendant failed to implement safety and security procedures and practices sufficient enough to protect from the data breach that it should have anticipated. Defendant should have known and anticipated that data breaches were on the rise, and that financial services institutions were lucrative or likely targets of cybercriminals looking to steal PII. Correspondingly, Defendant should have implemented and maintained procedures and practices appropriate to the nature and scope of information compromised in the data breach.

234. As a result of Defendant's violation of the Personal Information Protection Act, Plaintiffs Allen and Allen and the Illinois Subclass Members incurred economic damages, including expenses associated with necessary credit monitoring.

COUNT VII
VIOLATIONS OF ILLINOIS' SECURITY BREACH NOTIFICATION LAWS, 815 ILCS 530/10
(On Behalf of Plaintiffs Allen and Allen and Illinois Subclass Members)

235. Plaintiffs restate and reallege the foregoing Paragraphs 1 through 140 as if fully set forth herein.

236. Plaintiffs Allen and Allen bring this claim on behalf of themselves and the Illinois Subclass.

237. Defendant's conduct violated 815 ILCS 530/10, which requires entities to notify individuals "in the most expedient time possible and without unreasonable delay" in the event of a data breach.

238. The massive data breach occurred on or around July 19, 2021, however, notice of the data breach was not sent to Plaintiffs Allen and Allen and the Illinois Subclass Members until October 8, 2021.

239. Defendant unreasonably delayed informing anyone about the breach of security of Plaintiffs Allen and Allen and the Illinois Subclass Members' confidential and non-public information after Defendant knew the Data Breach had occurred.

240. Defendant failed to disclose to Plaintiffs or the Class Members, without unreasonable delay, and in the most expedient time possible, the breach of security of their unencrypted—or not properly and securely encrypted—PII when it knew or reasonably believed such information had been compromised.

241. As a result of Defendant's violation of 815 ILCS 530/10, Plaintiffs Allen and Allen and the Illinois Subclass Members incurred economic damages, including expenses associated with necessary credit monitoring.

COUNT VIII
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Subclasses)

242. Plaintiffs restate and reallege the foregoing Paragraphs 1 through 140 as if fully set forth herein.

243. This count is plead in the alternative to Count III (breach of implied contract).

244. Plaintiffs and Class Members conferred a monetary benefit on Defendant, by paying Defendant money, a portion of which was to have been used for data security measures to secure Plaintiffs' and Subclass Members' PII, and by providing Defendant with their valuable PII.

245. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Subclass Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiffs and Subclass Members by utilizing cheaper, ineffective security measures. Plaintiffs and Subclass Members, on the other hand,

suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

246. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Subclass Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

247. Defendant acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

248. If Plaintiffs and Subclass Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

249. Plaintiffs and Subclass Members have no adequate remedy at law.

250. As a direct and proximate result of Defendant's conduct, Plaintiffs and Subclass Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Subclass Members.

251. As a direct and proximate result of Defendant's conduct, Plaintiffs and Subclass Members have suffered and will continue to suffer other forms of injury and/or harm.

252. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Subclass Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Subclass Members overpaid for Defendant's services.

COUNT IX
Declaratory Judgment
(On Behalf of Plaintiffs and the Nationwide Class, or in the alternative, on behalf of the Subclass)

253. Plaintiffs restate and reallege all of the foregoing Paragraphs as if fully set forth herein.

254. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

255. Plaintiffs and Class Members entered into an implied contract that required Defendant to provide adequate security for the PII it collected from Plaintiffs and Class Members.

256. Defendant owes a duty of care to Plaintiffs and Class Members requiring them to adequately secure PII.

257. Defendant still possesses PII regarding Plaintiffs and Class Members.

258. Since the Data Breach, Defendant has announced few if any specific and significant changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent further attacks.

259. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and Class Members. In fact, now that Defendant's insufficient data

security is known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack.

260. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

261. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

262. Plaintiffs, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (2) that to comply with their contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of

Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant not transmit PII via unencrypted email;

f. Ordering that Defendant not store PII in email accounts;

g. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

h. Ordering that Defendant conduct regular computer system scanning and security checks;

i. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

j. Ordering Defendant to meaningfully educate their current, former, and prospective customers about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, requests judgment against the Timios and that the Court grant the following:

A. For an Order certifying the Nationwide Classes or, in the alternative, the Subclass as defined herein, and appointing Plaintiffs and their Counsel to represent the certified Classes;

B. For equitable relief enjoining Timios from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to the

Plaintiffs and Class members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and class members, including but not limited to an order:

i. prohibiting Timios from engaging in the wrongful and unlawful acts described herein;

ii. requiring Timios to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Timios to delete, destroy, and purge the personal identifying information of Plaintiffs and class members unless Timios can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and class members;

iv. requiring Timios to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiffs and class members' personal identifying information;

v. prohibiting Timios from maintaining Plaintiffs' and class members' personal identifying information on a cloud-based database;

vi. requiring Timios to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Timios's systems on a periodic basis, and ordering

Timios to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Timios to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Timios to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Timios to segment data by, among other things, creating firewalls and access controls so that if one area of Timios's network is compromised, hackers cannot gain access to other portions of Timios's systems;

x. requiring Timios to conduct regular database scanning and securing checks;

xi. requiring Timios to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and class members;

xii. requiring Timios to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Timios to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Timios's policies,

programs, and systems for protecting personal identifying information;

xiv. requiring Timios to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Timios's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Timios to meaningfully educate all class members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Timios to implement logging and monitoring programs sufficient to track traffic to and from Timios's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Timios's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

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

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: November 3, 2021

Respectfully Submitted,

/s/ M. Anderson Berry
M. ANDERSON BERRY (SBN 262879)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
(916) 777-7777
aberry@justice4you.com

Danielle L. Perry (SBN 292120)
MASON LIETZ & KLINGER LLP
5301 Wisconsin Avenue, NW. Suite 305
Washington, DC 20016
Tel: (202) 429-2290
dperry@masonllp.com

Attorneys for Plaintiffs and the Proposed Classes