UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
LONDON DIVISION

JONATHAN PHELPS, on behalf of himself and all others similarly situated, Plaintiff, v. **TOYOTETSU NORTH AMERICA,** Defendant.	**Case No: 6:22-cv-00106** **Judge Claria Horn Boom** **Magistrate Hanly A. Ingram** **JURY TRIAL DEMANDED**

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiff JONATHAN PHELPS ("Plaintiff") brings this First Amended Class Action Complaint against TOYOTETSU NORTH AMERICA ("Toyotetsu" or "Defendant"), as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant Toyotetsu a for-profit manufacturer of car components located in Somerset, Kentucky, to seek damages for himself and other similarly situated customers and current and former employees, or any other person(s) impacted in the data breach at issue ("Class Members") who he seeks to represent, as well as other equitable relief, including, without limitation, injunctive relief designed to protect the very sensitive information of Plaintiff and other Class Members. This action arises from Defendant's failure to properly secure and safeguard personal identifiable information, including without limitation, unencrypted and unredacted names, addresses, dates of birth, and Social Security

numbers (collectively, "personal identifiable information," "PII," or "Private Information").

2. Plaintiff alleges Defendant failed to provide timely, accurate and adequate notice to Plaintiff and Class Members who were or are customers or employees of Toyotetsu. Current and former customers and employees' knowledge about what personal identifiable information Toyotetsu lost, as well as precisely what types of information was unencrypted and in the possession of unknown third parties, was unreasonably delayed by Toyotetsu's unreasonable notification delay of four months after it first learned of the data breach.

3. On or about November 24, 2021, Toyotetsu notified state Attorneys General about a widespread data breach involving sensitive PII of 12,453 individuals.[1] Toyotetsu explained in its required notice letter that it discovered an unauthorized third-party gained access to a portion of Toyotetsu's network. Toyotetsu discovered that files on its network were accessed and acquired by the unknown actor (the "Data Breach").

4. In October 2021, Toyotetsu chose not to notify affected customers or employees or, upon information and belief, anyone of its data breach when it became aware of the situation, instead choosing to address the incident in-house by implementing other safeguards to some aspects of its computer security.

5. On November 24, 2021, Toyotetsu notified certain Class Members that their PII had been impacted and may have been taken from its network.[2]

6. According to Defendant, Toyotetsu alleges that it conducted "an investigation to determine what happened and whether any personal information was accessed or acquired without authorization as a result. Through the investigation, Toyotetsu learned that certain files containing

[1] Office of the Maine Attorney General, *Data Breach Notifications*, available at: https://apps.web.maine.gov/online/aeviewer/ME/40/275fde84-6559-4ed0-9ba4-a7a4a3d75dee.shtml (last accessed September 13, 2022).
[2] *Id.*

personal information may have been accessed or acquired without authorization."[3]

7. Toyotetsu alleges it "has taken steps in response to this incident to prevent similar incidents from occurring in the future."[4]

8. Toyotetsu further alleges it "remains dedicated to protecting personal information in its possession."[5]

9. Plaintiff and the Class Members in this action were, upon information and belief, current and former employees and current and former customers of Toyotetsu. Upon information and belief, the first that Plaintiff and the Class Members learned of the Data Breach was when they received by U.S. Mail Notice of Data Breach letters in November 2021.

10. In its notice letters, sent to Plaintiff and Class Members, Toyotetsu failed to explain why it took the company nearly two months to alert Class Members that their sensitive PII had been exposed. As a result of this delayed response, Plaintiff and Class Members were unaware that 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.

11. Plaintiff's and Class Members' unencrypted, unredacted PII was compromised due to Toyotetsu's negligent and/or careless acts and omissions, and due to the utter failure to protect Class Members' sensitive data. Hackers obtained their PII because of its value in exploiting and stealing the identities of Plaintiff and similarly situated Class Members. The risks to these persons will remain for their respective lifetimes.

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

---

[3] *Id.*
[4] *Id.*
[5] *Id.*

13. Plaintiff and Class Members have suffered injury as a result of Toyotetsu'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) the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits; deal with spam messages and e-mails received subsequent to the Data Breach, (v) charges and fees associated with fraudulent charges on their accounts, and (vi) the continued and certainly an increased risk to their PII, which remains in Toyotetsu's possession and is subject to further unauthorized disclosures so long as Toyotetsu fails to undertake appropriate and adequate measures to protect the PII. These risks will remain for the lifetimes of Plaintiff and Class Members.

14. Toyotetsu disregarded the rights of Plaintiff 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 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 Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff 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

15. Plaintiff Jonathan Phelps is, and at all times relevant has been, a resident and citizen of Kentucky, where he intends to remain. Plaintiff received a "Notice of Security" letter, dated November 24, 2021, on or about that date. The letter notified Plaintiff that on October 7, 2021, Toyotetsu identified unusual activity on its network and that "certain files containing personal

information may have been accessed or acquired without authorization." The type of data at issue included full names, dates of birth, addresses, and Social Security numbers. The letter further advised that Plaintiff that he could participate in credit monitoring services detecting suspicious activity.

16. Defendant Toyotetsu is Kentucky corporation headquartered in and with a principal office location of 100 Pin Oak Drive, Somerset, Kentucky 42503. Toyotetsu is a manufacturer of car components that was established in Somerset, Kentucky in 1995, and began production in 1997. Toyotetsu's customers include Toyota Motor Manufacturing Kentucky, Nissan, and Subaru.

17. 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 Plaintiff. Plaintiff 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.

18. All of Plaintiff's claims stated herein are asserted against Toyotetsu and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

19. 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 Class Member is a citizen of a state different from Defendant to establish minimal diversity.

20. The Eastern District of Kentucky has personal jurisdiction over Defendant named in this action because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conducts substantial business in Kentucky and this District through its headquarters, offices, parents, and affiliates.

21. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

22. Defendant is a manufacturer of car components that was established in Somerset, Kentucky with customers that include Toyota Motor Manufacturing Kentucky, Nissan, and Subaru.

23. Plaintiff and Class Members were customers and/or employees of Defendant whose PII was required to be provided, and was in fact provided, to Defendant in conjunction with manufacturing and purchase of car components or during the course of their employment with Defendant. Plaintiff's and Class Members' PII were required to fill out various forms, including without limitation employment paperwork and applications, tax documents, various authorizations, other form documents associated with the manufacturing of car components, and employment documentation.

24. Plaintiff and Class Members relied on the sophistication of Defendant and its network to keep their PII confidential and securely maintained, to use this information for business and/or employment purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

25. Defendant required the submission of and voluntarily accepted the PII as part of its business and had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Toyotetsu has a legal duty to keep employee and consumer PII safe and confidential.

26. The information held by Defendant in its computer systems and networks included the PII of Plaintiff and Class Members.

27. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII.

28. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Toyotetsu assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

29. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

30. In its Notice of Data Breach letter to victims of the Data Breach, Toyotetsu claims that it is dedicated to protecting personal information in its possession.[6]

31. Plaintiff and the Class Members, as current or former employees and/or customers of Toyotetsu, reasonably relied (directly or indirectly) on this sophisticated company to keep their sensitive PII confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their PII. Customers, in general, demand security to safeguard their PII, especially when sensitive PII is involved.

32. Toyotetsu had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

The Data Breach

33. "On October 7, 2021, Toyotetsu detected unusual network activity impacting certain systems."[7]

34. According to Defendant, Toyotetsu alleges that it conducted "an investigation to determine what happened and whether any personal information was accessed or acquired without authorization as a result. Through the investigation, Toyotetsu learned that certain files containing personal information may have been accessed or acquired without authorization." [8]

35. To date, Toyotetsu has not revealed when the unauthorized actor first gained access to a portion of Defendant's network, nor has it revealed the mechanism by which the unauthorized actor first gained access to Defendant's network.

36. Upon information and belief, the unauthorized actor gained access to Toyotetsu's network well in advance of the October 7, 2021, date that the intrusion was first discovered by Toyotetsu, meaning that the unauthorized actor had unfettered and undetected access to

[6] *Id.*
[7] *Id.*
[8] *Id.*

Defendant's networks for a considerable period of time prior to Toyotetsu becoming aware of the unauthorized access to its computer systems and network.

37. After Toyotetsu initially discovery the unauthorized access to its systems, Toyotetsu commissioned computer forensic specialists to conduct an investigation to determine the nature and scope of the event.

38. The investigation commissioned by Toyotetsu did not conclude until November 16, 2021, and notice was not sent to victims of the data breach at least a week after that. Thus, the victims of this Data Breach, including Plaintiff and Class Members, were not sent notice of this Data Breach until approximately eight weeks after Toyotetsu first knew about this Data Breach.

39. Defendant acknowledged that "certain files containing personal information may have been accessed or acquired without authorization."[9]

40. Defendant's investigation was inconclusive whether or not the accessed data has been or will be misused by the hackers. However, upon information and belief, Toyotetsu has no methods, policies, or procedures in place that would afford its employees and customers (like Plaintiff and Class Members) any mechanism or opportunity to report misuse of the data back to Toyotetsu, and the investigation commissioned by Toyotetsu did not survey individuals whose data was breached for evidence of misuse.

41. The attacker accessed, and likely acquired, files on the server containing PII, including names, addresses, dates of birth, and Social Security numbers.

42. On or around November 24, 2021, Defendant disclosed the Data Breach to the Maine Attorney General's Office. [10]

43. Toyotetsu first notified its impacted employees and consumers of the incident on or around November 24, 2021, sending written notifications to individuals whose personal information was compromised in the Data Breach.

44. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

---

[9] *Id.*
[10] *Id.*

45. Plaintiff further believes his PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the modus operandi of cybercriminals that commit cyber-attacks of this type.

46. Upon information and belief, the PII was not encrypted prior to the data breach.

47. Upon information and belief, the cyberattack was targeted at Toyotetsu as manufacturer that collects and maintains valuable personal, health, tax, and financial data from its current and former employees and customers.

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

49. In response to the Data Breach, Toyotetsu claims they has further secured their systems to protect the private information. Toyotetsu admits additional security was required, but there is no indication whether these steps are adequate to protect Plaintiff's and Class Members' PII going forward.

50. Toyotetsu had obligations created by contract, industry standards, common law, and representations made to customers and employees to keep the PII of Plaintiff and Class Members that was entrusted to Toyotetsu confidential, and to protect the PII from unauthorized access and disclosure.

51. Plaintiff and Class Members provided their PII to Toyotetsu with the reasonable expectation that Toyotetsu as a sophisticated company would comply with its duty and obligations and representations to keep such information confidential and secure from unauthorized access.

52. Toyotetsu failed to uphold its data security obligations to Plaintiff and Class Members. As a result, Plaintiff and Class Members are significantly harmed and will be at a high risk of identity theft and financial fraud for many years to come.

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

Securing PII and Preventing Breaches

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

55. In its notice letters, Toyotetsu acknowledged the sensitive and confidential nature of the PII. To be sure, collection, maintaining, and protecting PII is vital to virtually all of Toyotetsu's business purposes. Toyotetsu acknowledged through its 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

56. It is well known that PII, including Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

57. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[11]

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

59. Individuals are particularly concerned with protecting the privacy of their dates of birth and Social Security numbers, which are the "secret sauce" that is "as good as your DNA to hackers."

60. 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

[11] 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 December 10, 2021).

records, May 2020), Toyotetsu knew or should have known that its electronic records would be targeted by cybercriminals.

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

62. Despite the prevalence of public announcements of data breach and 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, Toyotetsu failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

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

63. At all relevant times, Toyotetsu had a duty to Plaintiff 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 Plaintiff and Class Members, and to *promptly* notify Plaintiff and Class Members when Toyotetsu became aware that their PII may have been compromised.

64. Toyotetsu's duty to use reasonable security measures arose as a result of the special relationship that existed between Toyotetsu, on the one hand, and Plaintiff and the Class Members, on the other hand. The special relationship arose because Plaintiff and the Members of the Class entrusted Toyotetsu with their PII when they were employees or customers of Toyotetsu.

65. Toyotetsu 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, Toyotetsu breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

66. 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.

67. 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]

68. The ramifications of Toyotetsu's failure to keep its Class Members' PII secure are long lasting and severe. Once PII is stolen, particularly a Social Security number, fraudulent use of that information and damage to victims is likely to continue for years.

The Value of Personal Identifiable Information

69. The PII of individuals remains of high value to criminals, as evidenced by the prices the criminals 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

[12] 17 C.F.R. § 248.201 (2013).
[13] *Id*.

$200, and bank details have a price range of $50 to $200.[14] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[15] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[16]

70. Social Security numbers, for example, are among the worst kind of PII 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 identity can cause a lot of problems.[17]

71. What is 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.

72. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link

---

[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/ (last visited Jan. 19, 2022).

[15] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Jan 19, 2022).

[16] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Jan. 19, 2022).

[17] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 19, 2022).

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]

73. 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. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—one's Social Security number.

74. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[19]

75. Among other forms of fraud, identity thieves may use Social Security numbers to obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

76. The fraudulent activity resulting from the Data Breach may not come to light for years.

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may

[18] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Jan. 19, 2022).

[19] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Nov. 11, 2021).

> continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[20]

78. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

79. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

80. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

81. In the breach notification letter, Defendant made an offer of twelve (12) months of credit and identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

82. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

83. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

---

[20] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Jan. 19, 2022).

Toyotetsu Failed to Comply with FTC Guidelines

84. Federal and State governments have established security standards and issued recommendations to lessen the risk of 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 reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[21]

85. 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.[22] 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.

86. 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 computer, a

[21] Federal Trade Commission, *Start With Security, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed December 10, 2021).

[22] 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 (last accessed December 10, 2021).

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.

87. The FTC has brought enforcement actions against businesses for failing to protect employee and customer 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.

88. Because Class Members entrusted Toyotetsu with their PII directly or indirectly, Toyotetsu had, and has, a duty to the Class Members to keep their PII secure.

89. Plaintiff and the other Class Members reasonably expected that when they provide PII to Toyotetsu, that Toyotetsu would safeguard their PII.

90. Toyotetsu was at all times fully aware of its obligation to protect the personal data of impacted individuals, including Plaintiff and members of the Classes. Toyotetsu was also aware of the significant repercussions if it failed to do so.

91. Toyotetsu's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data—including Plaintiff's and Class Members' full names, Social Security numbers, 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.

Plaintiff and Class Members Have Suffered Concrete Injury as a Result of Defendant's Inadequate Security and the Data Breach it Allowed.

92. Plaintiff and Class Members reasonably expected that Defendant would provide adequate security protections for their PII, and Class Members provided Defendant with sensitive personal information.

93. Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant for services, Plaintiff and other reasonable Class Members understood and expected that their PII would be protected with data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected. As such, Plaintiff and the Class Members suffered pecuniary injury.

94. 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. Plaintiff has 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.

95. 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, contact information, 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:

a. obtaining employment;

b. obtaining a loan;

c. applying for credit cards or spending money;

d. filing false tax returns;

e. stealing Social Security and other government benefits; and

f. applying for a driver's license, birth certificate, or other public document.

96. In addition, if a Class Member's Private Information 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.

97. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff 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.

98. 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.[23]

99. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class Members at an imminent, immediate, and

[23] *Id.*

continuing increased risk of identity theft and identity fraud.[24] Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[25] 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."[26] 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.

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

101. In its notice letter, Defendant represented to the Class Members and AGs that it initially was made aware of Data Breach in October 2021, and admitted files were accessed and acquired by the cybercriminals. As EmiSoft, an award-winning malware-protection software company, states "[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*."[27] It is likely that the cybercriminals did steal data and did so undetected.

102. In this case, according to Defendant's notification to the Class Members, cybercriminals had access to Class Members' data at least on October 7, 2021, yet its notice letters about that Data Breach did not go out until November 24, 2021. This is tantamount to the

---

[24] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (February 23, 2012), http://www.iii.org/insuranceindustryblog/?p=267 (last accessed December 10, 2021).

[25] 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 (last accessed December 10, 2021).

[26] 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) (last accessed December 10, 2021).

[27] 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/ (last accessed December 13, 2021, emphasis added)).

cybercriminals having an extended head start on stealing the identities of Plaintiff and Class Members.

103. Accordingly, that Defendant has admitted that the data was accessed, acquired, and stolen.

Plaintiff Jonathan Phelps's Experience

104. Plaintiff Phelps is a former Toyotetsu employee. He has not worked there since approximately 2013.

105. Plaintiff Phelps was required to provide and did provide his PII to Defendant during the course of his employment with Defendant. The PII included his name, address, date of birth, Social Security Numbers, driver's license number, telephone number, and other financial and tax information.

106. To date, Toyotetsu has done next to nothing to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this Data Breach.

107. Defendant's data breach notice letter downplays the theft of Plaintiff's and Class Members PII, when the facts demonstrate that the PII was targeted, accessed, and exfiltrated in a Data Breach. The fraud and identity monitoring services offered by Defendant are only for one year, and it places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for the service and addressing timely issues.

108. Plaintiff and Class Members have been further damaged by the compromise of their PII.

109. Plaintiff Phelps's PII was compromised in the Data Breach, and was likely stolen and in the hands of cybercriminals who illegally accessed Toyotetsu' network for the specific purpose of targeting the PII.

110. Plaintiff Phelps typically takes measures to protect his PII, and is very careful about sharing his PII. Phelps has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

111. Plaintiff Phelps stores any documents containing his PII in a safe and secure

location, and he diligently chooses unique usernames and passwords for his online accounts.

112. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. He monitors accounts and credit scores and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and duties.

113. Plaintiff has recently experienced fraudulent charges on a credit card account to which he is an authorized user, totaling approximately $300.00.

114. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant for the purpose of obtaining employment from Defendant, which was compromised in and as a result of the Data Breach.

115. Plaintiff 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. Since the Data Breach, Plaintiff has also experienced a significant increase in calls that can be characterized as spam or scams, receiving at times as many as 4 per day.

116. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security Number, being placed in the hands of criminals.

117. Defendant obtained and continues to maintain Plaintiff's PII (despite no longer having a legitimate use for it) and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Defendant required the PII from Plaintiff when he began employment with Defendant. Plaintiff, however, would not have entrusted his PII to Defendant had he known that it would fail to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

118. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of

identity theft and fraud for years to come.

119. Plaintiff Phelps has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Toyotetsu's possession, is deleted and/or protected and safeguarded from future breaches.

CLASS ALLEGATIONS

120. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated.

121. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> **All persons Toyotetsu North America identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

122. Excluded from the Classes are the following individuals and/or entities: Toyotetsu & Co, and Toyotetsu's parents, subsidiaries, affiliates, officers and directors, and any entity in which Toyotetsu 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.

123. Plaintiff reserves the right to modify or amend the definition of the proposed class and any future subclass before the Court determines whether certification is appropriate.

124. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are 12,453 individuals whose Private Information may have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

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

a. Whether and to what extent Defendant had a duty to protect Plaintiff's and Class

Members' Private Information;

b. Whether Defendant had duties not to disclose the Plaintiff's and Class Members' Private Information to unauthorized third parties;

c. Whether Defendant had duties not to use Plaintiff's and Class Members' Private Information for non-business purposes;

d. Whether Defendant failed to adequately safeguard Plaintiff's and Class Members' Private Information;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

h. Whether 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;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Private Information;

k. Whether Defendant violated the consumer protection statutes invoked herein;

l. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

m. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

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

126. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other

Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

127. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant 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. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

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

129. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): 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 Defendant. 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.

130. The nature of this action and the nature of laws available to Plaintiff and Class

Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant 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 Plaintiff 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.

131. The litigation of the claims brought herein is manageable. Defendant'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.

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

133. Unless a Class-wide injunction is issued, Defendant may continue in their failure to properly secure and unlawful disclosure of the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

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

135. 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 Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

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

d. Whether a contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that contract;

e. Whether Defendant breached the contract;

f. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

g. Whether Defendant breached the implied contract;

h. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

i. Whether 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;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Private Information;

k. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

136. Plaintiff restates and reallege all of the foregoing paragraphs as if fully set forth herein.

137. As a condition of being a employees or customers of Toyotetsu, individuals are obligated to provide Toyotetsu with certain PII, including but not limited to, their name, date of birth, address, Social Security number, state-issued identification numbers, tax identification numbers, military identification numbers, and financial account numbers.

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

139. Toyotetsu has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

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

141. Toyotetsu 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 Toyotetsu's security protocols to ensure that Plaintiff's and Class Members' information in Toyotetsu's possession was adequately secured and protected.

142. Toyotetsu also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII.

143. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of Toyotetsu's business as sophisticated manufacturer, for which the diligent protection of PII is a continuous forefront issue.

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

145. Toyotetsu's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Toyotetsu'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. Toyotetsu's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' PII, including basic encryption techniques freely available to Toyotetsu.

146. Plaintiff and Class Members had no ability to protect their PII that was in, and possibly remains in, Toyotetsu's possession.

147. Toyotetsu was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

148. Toyotetsu had and continues to have a duty to adequately and promptly disclose that the PII of Plaintiff and Class Members within Toyotetsu'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 Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

149. Toyotetsu had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and Class Members.

150. Toyotetsu has admitted that the PII of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

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

152. 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.

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

154. Toyotetsu improperly and inadequately safeguarded the PII of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

155. Toyotetsu failed to heed industry warnings and alerts to provide adequate safeguards to protect PII in the face of increased risk of theft.

156. Toyotetsu, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

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

158. But for Toyotetsu's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the PII of Plaintiff and Class Members would not have been compromised.

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

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

161. Toyotetsu 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. Toyotetsu'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 Plaintiff and Class Members.

162. Toyotetsu's violation of Section 5 of the FTC Act constitutes negligence *per se*.

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

164. 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 Plaintiff and Class.

165. As a direct and proximate result of Toyotetsu's negligence and negligence *per se*, Plaintiff 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 Toyotetsu's possession and is subject to further unauthorized disclosures so long as Toyotetsu fails to undertake appropriate and adequate measures to protect the PII 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 Plaintiff and Class Members; and (ix) the diminished value of Toyotetsu's goods and services they received.

166. As a direct and proximate result of Toyotetsu's negligence, 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.

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

COUNT II
Invasion of Privacy
(On Behalf of Plaintiff and the Nationwide Class)

168. Plaintiff re-alleges and incorporates by reference the above paragraphs as if fully set forth herein.

169. Plaintiff and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

170. Defendant owed a duty to its current and former employees, including Plaintiff and Class Members, to keep their PII contained as a part thereof, confidential.

171. Defendant failed to protect and released to unknown and unauthorized third parties the PII of Plaintiff and Class Members.

172. Defendant has acted with reckless disregard for the privacy of Plaintiff and Class Members rising to the level of (1) an intentional intrusion by Defendant, (2) into a matter that Plaintiff and Class Members have a right to keep private (i.e., their PII), and (3) which is highly offensive to a reasonable person.

173. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it had actual knowledge that its information security practices were inadequate

and insufficient. For example, Defendant knew that PII was stored for years after Defendant no longer had a legitimate use for such data. Defendant also knew that the PII it stored was not securely encrypted, and that its systems were vulnerable to foreseeable threats as a result of inadequate security measures and training.

174. Moreover, upon information and belief, the Data Breach was the result of a phishing attack, which both Defendant's security software and Defendant's employees should have recognized, as this is the most common method of effectuating a data breach.[28] By revealing necessary credentials to access the system or network storing Plaintiff's and Class Members' PII in response to a phishing attack, Defendant actively disclosed Plaintiff's and Class Members' PII and invaded their privacy.

175. As discussed in this Complaint, Defendant was aware of the potential of a data breach and failed to adequately safeguard its systems and implement appropriate policies to prevent the unauthorized release of Plaintiff's and Class Members' data.

176. Defendant acted with such reckless disregard as to the safety of Plaintiff's and Class Members' PII to rise to the level of intentionally allowing the intrusion upon Plaintiff's and Class Members' seclusion.

177. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and the Class Members is highly offensive to a reasonable person.

178. Plaintiff and Class Members have been damaged by the invasion of their privacy in an amount to be determined at trial.

---

[28] *See* https://en.wikipedia.org/wiki/Phishing ("As of 2020, phishing is by far the most common attack performed by cybercriminals, the FBI's Internet Crime Complaint Centre recording over twice as many incidents of phishing than any other type of computer crime.") (citing *Internet Crime Report 2020*, FBI Internet Crime Complaint Centre. U.S. Federal Bureau of Investigation. Retrieved 21 March 2021); *see also* https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/ (last visited Sept. 16, 2022) ("Phishing is the most common type of social engineering, which is a general term describing attempts to manipulate or trick computer users. Social engineering is an increasingly common threat vector used in almost all security incidents. Social engineering attacks, like phishing, are often combined with other threats, such as malware, code injection, and network attacks.").

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

179. Plaintiff re-alleges and incorporate by reference paragraphs above as if fully set forth herein.

180. Defendant collected, maintained, and stored the PII of Plaintiff and Class Members and, as such, Defendant had knowledge of the benefits it received on behalf of the Plaintiff and Class Members.

181. Defendant also understood and appreciated that Plaintiff's and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

182. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of employment or purchasing products from Defendant, and in connection thereto, by providing their PII to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically, they were required to provide Defendant with their PII. In exchange, Plaintiff and Class Members should have received adequate protection and data security for such PII held by Defendant.

183. Defendant knew Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

184. Defendant failed to provide reasonable security, safeguards, and protections to the PII of Plaintiff and Class Members.

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

186. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

187. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

188. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

189. Plaintiff re-alleges and incorporates by reference the foregoing paragraphs as if fully set forth herein.

190. This count is plead in the alternative to Count II (Unjust Enrichment) above.

191. Plaintiff's and Class Members' PII was provided to Defendant as part of employment or manufacturer services that Defendant provided to Plaintiff and Class Members.

192. Plaintiff and Class Members agreed to pay Defendant for its products.

193. Defendant and the Plaintiff and Class Members entered into implied contracts for the provision of adequate data security, separate and apart from any express contracts concerning the security of Plaintiff's and Class Members' PII, whereby, Defendant was obligated to take reasonable steps to secure and safeguard Plaintiff's and Class Members' PII.

194. Defendant had an implied duty of good faith to ensure that the PII of Plaintiff and Class Members in its possession was only used in accordance with its contractual obligations.

195. Defendant was therefore required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiff's and Class Members' PII and to comply with industry standards and applicable laws and regulations for the security of this information.

196. Under these implied contracts for data security, Defendant was further obligated to provide Plaintiff and all Class Members, with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII.

197. Defendant breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiff's and Class Members' PII, resulting in the Data Breach.

198. Defendant further breached the implied contract by providing untimely notification to Plaintiff and Class Members who may already be victims of identity fraud or theft or are at present risk of becoming victims of identity theft or fraud.

199. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

200. As a result of Defendant's conduct, Plaintiff and Class Members did not receive the full benefit of the bargain.

201. Had Defendant disclosed that its data security was inadequate, neither the Plaintiff or Class Members, nor any reasonable person would have entered into such contracts with Defendant.

202. As a result of Data Breach, Plaintiff and Class Members suffered actual damages resulting from the theft of their PII, as well as the loss of control of their PII, and remain at present risk of suffering additional damages.

203. Plaintiff 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.

204. Plaintiff 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.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, requests judgment against Defendant Toyotetsu and that the Court grant the following:

A. For an Order certifying the Nationwide Classes and appointing Plaintiff and his Counsel to represent the certified Nationwide Class;

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

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

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

ii. requiring Toyotetsu 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 Toyotetsu to delete, destroy, and purge the personal identifying information of Plaintiff and Class unless Toyotetsu can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and the Class;

iv. requiring Toyotetsu to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff's and Class Members' personal identifying information;

v. prohibiting Toyotetsu from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

vi. requiring Toyotetsu 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 Toyotetsu's systems on a periodic basis, and ordering Toyotetsu to promptly correct any problems or issues detected by such third-party security auditors;

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

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

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

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

xi. requiring Toyotetsu 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 Plaintiff and Class Members;

xii. requiring Toyotetsu 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 Toyotetsu 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 Toyotetsu's policies, programs, and systems for protecting personal identifying information;

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

updated;

xv. requiring Toyotetsu 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 Toyotetsu to implement logging and monitoring programs sufficient to track traffic to and from Toyotetsu'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 Toyotetsu'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, 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

Plaintiff hereby demands that this matter be tried before a jury.

Date: September 16, 2022

Respectfully Submitted,

/s/ Terence R. Coates

Terence R. Coates (*Pro Hac Vice*)
Jonathan T. Deters (*Pro Hac Vice* forthcoming)
Dylan J. Gould (*Pro Hac Vice* forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219

tcoates@msdlegal.com
jdeters@msdlegal.com
dgould@msdlegal.com

Joseph B. Venters
VENTERS LAW OFFICE
P.O. Box 1749
Somerset, KY 42502
606-451-0332/606-451-0335
joey@venterslaw.com

Attorneys for Plaintiff and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that on September 16, 2022, I served a copy of the foregoing via electronic filing in the ECF system.

/s/ Terence R. Coates
Terence R. Coates (*Pro Hac Vice*)