

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION**

Bruce Narolis, *individually and on
behalf of all others similarly situated,*

Plaintiff,

v.

Doxim, Inc.,

Defendant.

Case No. _____

**CLASS ACTION
COMPLAINT**

JURY TRIAL DEMANDED

Plaintiff Bruce Narolis (“Plaintiff”), individually and on behalf of all others similarly situated (the “Class” or “Class Members”), brings this Class Action Complaint (the “Complaint”) against Defendant Doxim, Inc. (“Defendant”). The allegations set forth in this Complaint are based on the personal knowledge of the Plaintiff and upon information and belief and further investigation of counsel.

I. NATURE OF THE ACTION

1. This is a data breach class action against Defendant for its failure to adequately secure and safeguard confidential and sensitive information held throughout the typical course of business of Plaintiff and the Class.

2. On or about December 30, 2023, an unauthorized actor gained access to the Defendant's network and computer systems and obtained unauthorized access to Defendant's files. (the "Data Breach").

3. Upon information and belief, thousands of individuals' information was affected by the Data Breach. The information exposed or otherwise accessed by an unauthorized third-party in the Data Breach included Plaintiff and the Class member's names, addresses, financial account numbers, and social security numbers ("SSN").¹ Collectively, the information described in this paragraph shall be referred to as "PII" (Personally Identifiable Information) throughout this Complaint.

4. Defendant learned of the suspected Data Breach on or about December 30, 2023.

5. According to Defendant, after learning of the incident, it conducted an investigation and engaged outside cybersecurity professionals and data privacy counsel. Defendant, so far, has yet to inform affected individuals when it completed its investigation or when it completely learned the extent of the Data Breach.

6. On or about May 31, 2024, Defendant notified affected individuals that their PII was impacted in the Data Breach.²

¹ See Notice of Security Incident Dated May 31, 2024, effectively known as "The Notice."

² *Id.*

7. On information and belief, Defendant notified at least some of its direct customers prior to notifying Plaintiff and other affected Class members, including, e.g., notifying Truliant Federal Credit Union (based in North Carolina) on April 22, 2024. Further, on May 29, 2024, Truliant Federal Credit Union made a public statement regarding the data of some of its customers which was in the possession of Defendant and had been compromised.

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

9. Plaintiff and the Class have taken reasonable steps to maintain the confidentiality and security of their PII.

10. Plaintiff and the Class reasonably expected Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

11. Defendant, however, breached its numerous duties and obligations by failing to implement and maintain reasonable safeguards; failing to comply with industry-standard data security practices and federal and state laws and regulations governing data security; failing to properly train its employees on data security measures and protocols; failing to timely recognize and detect unauthorized third

parties accessing its system and that substantial amounts of data had been compromised; and failing to timely notify the impacted Class.

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

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

14. Plaintiff and the Class are now faced with a present and imminent lifetime risk of identity theft or fraud. These risks are made more substantial, and significant because of the inclusion of their SSN and other static PII.

15. PII has great value to cyber criminals, especially an individuals' SSN. As a direct cause of Defendant's Data Breach, Plaintiff's, and the Class's PII is in the hands of cyber-criminals and may be available for sale on the dark web for other criminals to access and abuse at the expense of Plaintiff and the Class. Plaintiff and the Class face a current and lifetime risk of identity theft or fraud as a direct result of the Data Breach.

16. Defendant acknowledges the imminent threat the Data Breach has caused to Plaintiff.³

17. The modern cyber-criminal can use the PII and other information stolen in cyber-attacks to assume a victim's identity when carrying out various crimes such as:

- a. Obtaining and using a victim's credit history;
- b. Making financial transactions on their behalf and without their knowledge or consent, including opening credit accounts in their name or taking out loans;
- c. Impersonating them in written communications, including mail e-mail and/or text messaging;
- d. Stealing, applying for and/or using benefits intended for the victim;
- e. Committing illegal acts while impersonating their victim which, in turn, could incriminate the victim and lead to other legal ramifications.

18. Plaintiff's and Class members' PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect Plaintiff's and Class members' PII. Defendant not only failed to prevent the Data Breach, but after discovering the Data Breach in December 2023, Defendant waited

³ See *gen. n.1.*

until on or around May 31, 2024, to notify affected individuals such as Plaintiff and members of the Class.

19. As a result of Defendant's delayed response to the data breach, Plaintiff and the Class had no idea their PII had been compromised, and that they were, and continue to be, at significant and imminent risk of identity theft, fraud, and various other forms of personal, social and financial harm. The risk will remain for their respective lifetimes because of Defendant's negligence.

20. Plaintiff brings this action on behalf of all persons whose PII was compromised in the Data Breach as a direct consequence for Defendants failure to:

- (i) adequately protect consumers' PII entrusted to it,
- (ii) warn its current and former customers, potential customers, and current and former employees of their inadequate information security practices, and
- (iii) effectively monitor their websites and platforms for security vulnerabilities and incidents.

Defendant's conduct amounts to negligence and violates federal and state statutes and guidelines.

21. As a result of the Data Breach, Plaintiff and the Class suffered ascertainable losses, including but not limited to, a loss of privacy. These injuries include:

- (i) the invasion of privacy;
- (ii) the compromise, disclosure, theft, and imminent unauthorized use of Plaintiff's and the Class's PII;
- (iii) emotional distress, fear, anxiety, nuisance and annoyance related to the theft and compromise of their PII;
- (iv) lost or diminished inherent value of PII; out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time or wages;
- (v) the continued and increased risk to their PII, which, (a) remains available on the dark web for individuals to access and abuse; and (b) remains 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 Plaintiff and the Class.

22. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose PII was

compromised and stolen as a result of the Data Breach and remains at risk due to inadequate data security practices employed by Defendant.

23. Accordingly, Plaintiff, on behalf of himself and the Class, asserts claims for Negligence, Negligence *Per Se*, and Unjust Enrichment. Plaintiff seeks injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity by law, or any other relief the Court deems just and appropriate.

II. PARTIES

24. Plaintiff Bruce Narolis is, and at all relevant times was, a citizen of Morganton, North Carolina.

25. Plaintiff received a Letter from his bank, Truiliant Federal Credit Union, on or about May 14, 2024, informing Plaintiff of Defendant's Data Breach. Upon information and belief, Defendant did not notify all Class Members and affected individuals until on or about May 31, 2024.

26. The Letter advised Plaintiff that an unauthorized third party could have accessed his personal information. This information included his name, account number, and SSN. The same is true for the Notice sent to all Class Members.⁴

27. Prior to this Data Breach, Plaintiff had taken steps to protect and safeguard his PII including monitoring his PII closely. He has not knowingly transmitted his PII over unsecured or unencrypted internet connections.

⁴ See n.1.

28. Defendant was founded in 2000.⁵ Defendant provides customer communications management and engagement technology solutions to highly regulated organizations, enhancing digitization, operational efficiency, and customer experience.⁶

29. Upon information and belief, Defendant is headquartered in Canada, with a major office at 1911 Woodslee Drive, Troy, Michigan 48083.

30. Defendant collected and continues to collect the PII of its customers and clients throughout its usual course of business operations.

31. Defendant's privacy policy provides that, among other things, "Your personal information is kept securely in line with physical, technical, and administrative security measures" and "We endeavor to comply with applicable data privacy laws in the jurisdictions in which we operate."⁷

32. By obtaining, collecting, using, and deriving benefit from Plaintiff's and Class members' PII, Defendant assumed legal and equitable duties to those persons, and knew or should have known that it was responsible for protecting Plaintiff's and Class's PII from unauthorized disclosure and/or criminal cyber activity that would lead to readily foreseeable harm to Plaintiff and the Class.

⁵ <https://www.doxim.com/about-us/>.

⁶ *Id.*

⁷ <https://www.doxim.com/privacy-policy/>.

III. JURISDICTION AND VENUE

33. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d), *et seq.* The amount in controversy exceeds \$5 million, exclusive of interest and costs. There are more than 100 members in the proposed Class, and at least one member of the Class, including Plaintiff, is a citizen of a state different from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

34. This Court has personal jurisdiction over Defendant because Defendant has a substantial presence in this District and is a citizen of a foreign state. Defendant has substantial contacts with the forum.

35. Venue is proper in this Court under 28 U.S.C. § 1391, because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District, and Defendant resides within this judicial district.

IV. FACTUAL ALLEGATIONS

A. Background

36. In the ordinary course of its business practices, Defendant stores, maintains, and uses an individuals' PII, which includes Plaintiff and Class Members', including but not limited to information such as:

- a. Full names;

- b. Personal home address;
- c. Private financial account information; and
- d. Social Security numbers;

37. Defendant understands the importance of securely storing and maintaining PII.

B. The Data Breach

38. Defendant became aware of the Data Breach on or about December 30, 2023.⁸

39. Defendant then made steps to secure its systems and network including retaining independent cybersecurity experts to investigate the matter further but neglected to notify all affected individuals of the Data Breach quickly and appropriately until on or about May 31, 2024.

40. Additionally, though Plaintiff and the Class have an interest in ensuring that their information remains protected, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures taken by Defendant to ensure a data breach does not occur again, have not been shared with regulators, Plaintiff, or Members of the Class.

⁸ See n.1.

C. Defendant Was Aware of the Data Breach Risks

41. Considering recent high-profile data breaches at other companies in the financial industry, Defendant knew or should have known that their electronic records would be targeted by cybercriminals.

42. The financial industry has endured over 20,000 cyberattacks in the past two decades, leading to losses exceeding \$12 billion.”⁹ Additionally, the losses are most substantial and impactful at smaller financial institutions, likely due to their less robust data security systems.¹⁰

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

44. Defendant had and continues to have obligations created by implied contract, industry standards, common law, and representations made to Plaintiff and the Class, to keep their PII private and confidential and to protect it from unauthorized access, disclosure, or exfiltration.

45. Plaintiff and the Class provided their PII to Defendant with the reasonable expectation that an entity such as Defendant, which is responsible for

⁹ Fabio Natalucci, *Rising Cyber Threats Pose Serious Concerns for Financial Stability*, IMF Blog (April 9, 2024), <https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability> (last visited June 12, 2024).

¹⁰ *Id.*

maintaining customer data, would comply with their obligations to employ reasonable care to keep such information confidential and secure from unauthorized access.

46. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and data breaches in the banking, credit, and financial service industries preceding the date of the Data Breach, particularly considering Defendant's role in that industry.

47. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and foreseeable to the public and to anyone in Defendant's industry, including Defendant.

48. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take substantial time, money, and patience to resolve.¹¹ Identity thieves use the stolen PII

¹¹ See *Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), <https://www.myoccu.org/sites/default/files/pdf/taking-charge-1.pdf> (last visited June 10, 2024).

for a variety of crimes, including but not limited to, credit card fraud, telephone or utilities fraud, and bank and finance fraud.¹²

49. The PII of Plaintiff and the Class were accessed and taken by cyber criminals for the very purpose of engaging in illegal and unethical conduct, including crimes involving identity theft, fraud, or to otherwise profit by selling their data to other criminals who purchase PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

50. Defendant knew, or reasonably should have known, of the critical importance of safeguarding the Plaintiff's and Class members' PII, including their Social Security Numbers (SSNs) and financial details. The Defendant also knew, or should have known, the foreseeable consequences of a breach in their data security systems, which would specifically lead to significant costs and damages for the Plaintiff and the Class.

51. Plaintiff and the Class now face years of constant monitoring and surveillance of their financial and personal records. The Class is incurring and will

¹² *Id.* The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” 16 CFR § 603.2. 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.” *Id.*

continue to incur such damages in addition to any fraudulent use of their PII as a direct result of the Data Breach.

52. The injuries to Plaintiff and Class members were directly and proximately caused by Defendant's own failure to install, implement, or maintain adequate data security measures, software and other industry best practices for safeguarding the PII of Plaintiff and the Class.

D. Defendant Failed to Comply with FTC Guidelines

53. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable and adequate data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

54. In 2022, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of

data being transmitted from the system; and have a response plan ready in the event of a breach.¹³

55. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

56. The FTC has brought enforcement actions against businesses for failing to protect 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.

57. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against

¹³ Ritchie, J. N. & A., & Jayanti, S.F.-T. and A. (April 26, 2022). *Protecting personal information: A guide for business*. Federal Trade Commission. https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed June 10, 2024)

unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

58. To prevent and detect cyber-attacks, including the cyber-attack on Defendants network that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government and FTC, the following measures:

- a. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of malware and how it is delivered;
- b. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing;
- c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users;
- d. Configure firewalls to block access to known malicious IP addresses;

- e. Patch operating systems, software, and firmware on devices using a centralized patch management system;
- f. Set anti-virus and anti-malware programs to automatically conduct regular scans and/or repairs;
- g. Create and manage the use of privileged accounts based on the varying level of accessibility using a principle of least privilege: wherein no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary, such as any internal IT employees;
- h. Configure access controls—including file, directory, and network share permissions— with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares;
- i. Disable macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications;
- j. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common malware

locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder;

- k. Consider disabling Remote Desktop protocol (RDP) if it is not being used;
- l. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy;
- m. Execute operating system environments or specific programs in a virtualized environment; and
- n. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

59. Defendant was at all times fully aware of its obligation to protect the PII of its clients' customers, prospective customers, and employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

E. Defendant Failed to Comply with Industry Standards

60. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices. Best cybersecurity practices that are standard in the financial services industry include installing appropriate malware

detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points of security.

61. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity 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 established standards in reasonable cybersecurity readiness. These frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

62. The occurrence of the Data Breach is indicative that Defendant failed to adequately implement one or more of the above measures to prevent or circumvent ransomware attacks or other forms of malicious cybercrimes, resulting in the Data Breach.

F. PII Holds Value to Cyber Criminals

63. Businesses, such as Defendant, that store PII in their daily course of business are more likely to be targeted by cyber criminals. Credit card, routing, bank account and other financial numbers are highly sought data targets for hackers, but information such as date of birth, driver's license number, and SSN are even more desirable to cyber criminals; they are not easily destroyed or replaceable and can be easily used to perpetrate acts of identity theft and other types of fraud.

64. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web to obtain PII of other unknown individuals. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from \$40 to \$200, and banking details have a price range of \$50 to \$200.¹⁴

65. A person's SSN, for example, is among the worst kind of PII to have stolen or otherwise compromised because they may be put to a variety of fraudulent uses and are difficult for an individual to change or otherwise repair once it's compromised. The Social Security Administration ("SSA") 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:

¹⁴ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, (Oct. 16, 2019), <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited June 10, 2024).

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.¹⁵

66. What is more, it is no easy task to change or cancel a stolen or compromised Social Security number as is the case for several of the Class members in this action. An individual cannot obtain a new SSN without significant time, monetary investment, paperwork, and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of an SSN is not permitted and the only form of remediation happens *after* the first incident of misuse; an individual must show evidence of actual, ongoing fraudulent activity to be eligible to submit an application requesting a new SSN with the SSA.

67. Furthermore, as the SSA warns:

Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit

¹⁵ *Identity Theft and Your Social Security Number*, <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed June 10, 2024).

record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.

If you receive a new Social Security Number, you should not be able to use the old number anymore.

For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.¹⁶

68. Here, the unauthorized access by cyber criminals left them with the tools to perform the most thorough identity theft—they have obtained enough of the essential PII that can be used to mimic the identity of the victim. The PII of Plaintiff and the Class stolen in the Data Breach constitutes a dream for hackers or cyber criminals and a nightmare for Plaintiff and the Class. Stolen personal data of Plaintiff and the Class represents essentially one-stop shopping for identity thieves indefinitely.

69. The FTC has released its updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

¹⁶ *Id.*

70. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office (“GAO”) Report to Congressional Requesters:

[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 continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.¹⁷

71. Companies recognize that PII is a valuable asset and a valuable commodity, but also necessary throughout the typical course of business with consumers. A “cyber black-market” exists in which criminals openly post stolen SSN and other PII on several dark web Internet websites. The stolen PII of Plaintiff and the Class has a high value on both legitimate and black markets.

72. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver’s license or identification card in the victim’s name but with another’s picture, and/or using the victim’s information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

¹⁷ See <https://www.gao.gov/assets/gao-07-737.pdf> (June 2007) at 29.

73. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use SSNs to create false bank accounts or file fraudulent tax returns or other tax related forms and documents using an alias of their victim. Class members whose SSN have been compromised in the Data Breach now face a real, present, imminent, and substantial risk of identity theft and other problems associated with the disclosure of their SSN and will need to monitor their credit and tax filings for an indefinite duration.

74. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, merely losing payment information in a retailer data breach, because those victims can file disputes, cancel or close credit and debit cards and/or accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not nearly impossible, to change.

75. 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.”¹⁸

¹⁸ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), <https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited June 10, 2024).

76. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police or other emergency medical services. An individual may not know that their driver's license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

G. Plaintiff's and Class Members' Damages

77. Defendant has failed to provide any compensation for the unauthorized release and disclosure of Plaintiff's and the Class's PII.

78. Plaintiff and the Class have been damaged by the compromise of their PII in the Data Breach.

79. Plaintiff and the Class presently face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

80. Plaintiff and the Class have been, and currently face substantial risk of being targeted now and in the future, for phishing schemes, data intrusion, and other illegality based on their PII being compromised in the Data Breach as potential fraudsters could use the information garnered to target such schemes more effectively against Plaintiff and the Class.

81. Plaintiff and the Class may also incur out-of-pocket costs for implementing protective measures such as purchasing credit monitoring fees, credit report fees, credit freeze fees, and other similar costs directly or indirectly related to the Data Breach.

82. Plaintiff and the Class also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in data breach cases.

83. Plaintiff and the Class have spent and will continue to spend significant amounts of uncompensated time to monitor their financial accounts, medical accounts, sensitive information, credit score, and records for misuse.

84. Plaintiff and the Class have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach

85. Moreover, Plaintiff and the Class have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of proper and adequate security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password protected.

86. Further, because of Defendant's conduct, Plaintiff and the Class are forced to live with the anxiety and fear that their PII—which contains the most intimate details about a person's life—may be disclosed to the entire world, whether physically or virtually, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

87. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and the Class have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm because of the Data Breach.

H. Plaintiff Bruce Narolis's Experience

88. Plaintiff, through his credit union, entrusted his PII and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to his PII. Plaintiff would not have allowed Defendant to collect and maintain his PII had he known that Defendant would not take reasonable steps to safeguard his PII.

89. Plaintiff has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone calls to obtain more information about the Data Breach and researching

the Data Breach. This is uncompensated time that has been lost forever and cannot be recaptured.

90. Plaintiff stores all documents containing his PII in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for the online accounts that he has.

91. Plaintiff has suffered actual injury in the form of damages to, and diminution in, the value of his PII – a form of intangible property that Plaintiff entrusted to Defendant. This PII was compromised in, and has been diminished as a result of, the Data Breach.

92. Plaintiff has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

93. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII resulting from the compromise of his PII, especially his SSN, in combination with his name, which is now in the hands of cyber criminals and other unauthorized third parties.

94. Knowing that thieves stole his PII, including his SSN, and knowing that his PII will likely be sold on the dark web, has caused Plaintiff great anxiety.

95. Plaintiff has a continuing interest in ensuring that his PII which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches.

96. As a result of the Data Breach, Plaintiff is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

V. CLASS ACTION ALLEGATIONS

97. Plaintiff brings this nationwide class action according to Federal Rules of Civil Procedure, Rules 23(b)(2), 23(b)(3), and 23(c)(4).

98. The nationwide Class that Plaintiff seeks to represent is defined as follows:

All persons residing in the United States whose PII was compromised during the Data Breach that is the subject of the Notice of Data Breach published by Defendant in May 2024 (the “Class”).

99. Excluded from the Class are: (i) Defendant and its employees, officers, directors, affiliates, parents, subsidiaries, and any entity in which Defendant has a whole or partial ownership of financial interest; (ii) all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; (iii) any counsel and their respective staff appearing in this matter; and (iv) all judges assigned to hear any aspect of this litigation, their immediate family members, and their respective court staff.

100. Plaintiff reserves the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

101. **Numerosity.** The Class is so numerous that joinder of all members is impracticable. The Class likely includes, at the least, thousands of individuals whose personal data was compromised by the Data Breach. The exact number of Class members is in the possession and control of Defendant and will be ascertainable through discovery.

102. **Commonality.** There are numerous questions of law and fact common to Plaintiff and the Class that predominate over any questions that may affect only individual Class members, including, without limitation:

- a. Whether Defendant unlawfully maintained, lost or disclosed Plaintiff's and the Class's PII;
- b. 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;
- c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

- e. Whether Defendant owed a duty to Class to safeguard their PII;
- f. Whether Defendant breached duties to Class to safeguard their PII;
- g. Whether cyber criminals obtained Class's PII in the Data Breach;
- h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- i. Whether Defendant owed a duty to provide Plaintiff and Class timely notice of this Data Breach, and whether Defendant breached that duty;
- j. Whether Plaintiff and Class suffered legally cognizable damages as a result of Defendant's misconduct;
- k. Whether Defendant's conduct was negligent;
- l. Whether Defendant's conduct violated federal law;
- m. Whether Defendant's conduct violated state law; and
- n. Whether Plaintiff and Class are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

103. **Typicality.** Plaintiff's claims are atypical of the claims of the Class in that Plaintiff, like all proposed Class members, had his PII compromised, breached, or otherwise stolen in the Data Breach. Plaintiff and the Class were injured through the uniform misconduct of Defendant, described throughout this Complaint, and assert the same claims for relief.

104. **Adequacy.** Plaintiff and counsel will fairly and adequately protect the interests of Plaintiff and the proposed Class. Plaintiff retained counsel who are experienced in Class action and complex litigation, particularly those involving Data Breach as is at issue in this class action complaint. Plaintiff has no interests that are antagonistic to, or in conflict with, the interests of other Class members.

105. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiff and the Class have been harmed by Defendant's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct and/or inaction. Plaintiff knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

106. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A), in that the prosecution of separate actions by the individual Class members would create a risk of inconsistent or varying adjudications with respect to individual

members of the Class, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each member of the Class. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing Defendant to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by Class members would create the risk of adjudications with respect to individual Class members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

107. Class certification, therefore, is appropriate under Rule 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

108. 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 its legal duty or obligation to Plaintiff and the Class to exercise due care in collecting, storing, using, safeguarding, or otherwise maintaining their PII;
- b. Whether Defendant breached its legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, safeguarding, or otherwise maintaining their PII;
- c. Whether Defendant failed to comply with its own policies or procedures and applicable laws, regulations, and industry standards relating to data security;
- d. 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; and
- e. Whether Plaintiff and the Class are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

VI. CAUSES OF ACTION

COUNT I

Negligence

(On behalf of Plaintiff and the Class)

109. Plaintiff and the Class re-allege and incorporate all foregoing paragraphs.

110. Plaintiff and the Class, through their financial institutions or other clients of Defendant, entrusted Defendant with their PII.

111. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and not disclose their PII to unauthorized third parties. Had Plaintiff and the Class known their PII would not be protected, they would not have allowed Defendant to possess it.

112. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining, using, maintaining, and protecting their PII from unauthorized third parties.

113. The legal duties owed by Defendant to Plaintiff and the Class include, but are not limited to the following:

- a. To exercise reasonable care in procuring, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiff and the Class in Defendant's possession;
- b. To protect PII of Plaintiff and the Class in Defendant's possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

- c. To implement processes and software to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Class of the Data Breach.

114. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the Federal Trade Commission, the unfair practices by companies such as Defendant of failing to use reasonable measures to protect PII.

115. Various FTC publications and data security breach orders further form the basis of Defendant's duty. Plaintiff and Class are consumers under the FTC Act. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and by not complying with industry standards.

116. Defendant breached its duties to Plaintiff and the Class. Defendant knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the fact that data breaches have recently been prevalent.

117. Defendant knew or should have known that its security practices did not adequately safeguard the PII of Plaintiff and the Class.

118. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security measures and its failure to protect the PII of Plaintiff and the Class from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiff and the Class during the period it was within Defendant's possession and control.

119. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Defendant was entrusted with Plaintiff's and Class members' confidential PII.

120. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and the Class.

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

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

123. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Class.

124. Defendant breached the duties it owes to Plaintiff and Class in several ways, including:

- a. Failing to implement adequate security systems, protocols, and practices sufficient to protect employees' and customers' PII and thereby creating a foreseeable risk of harm;
- b. Failing to comply with the minimum industry data security standards during the period of the Data Breach;
- c. Failing to act despite knowing or having reason to know that its systems were vulnerable to attack; and
- d. Failing to timely and accurately disclose to customers and employees that their PII had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

125. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was stolen and accessed as the proximate result of Defendant's failure

to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

126. Due to Defendant's misconduct, Plaintiff and the Class are entitled to credit monitoring at a minimum. The PII taken in the Data Breach can be used for identity theft and other types of financial fraud against Plaintiff and the Class.

127. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately \$219 to \$358 per year.¹⁹

128. As a result of Defendant's negligence, Plaintiff and Class suffered injuries that include:

- i. the 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

¹⁹ See, Kiah Treece, *Best Credit Monitoring Services of June 2024*, Forbes Advisor, [https://www.forbes.com/advisor/credit-score/best-credit-monitoring-services/#:~:text=Prices%20range%20from%20%248.99%20to,k\)%20plans%20and%20other%20investments](https://www.forbes.com/advisor/credit-score/best-credit-monitoring-services/#:~:text=Prices%20range%20from%20%248.99%20to,k)%20plans%20and%20other%20investments) (last visited June 11, 2024)

not limited to, time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account;

- iv. the continued risk to their PII, which may remain for sale on the dark web and is in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession;
- v. future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class, including ongoing credit monitoring.

129. These injuries were reasonably foreseeable given the history and uptick of data security breaches of this nature within the financial sector. The injury and harm that Plaintiff and the Class suffered was the direct and proximate result of Defendant's negligent conduct.

COUNT II
Negligence *Per Se*
(On behalf of Plaintiff and the Class)

130. Plaintiff and the Class re-allege and incorporate all foregoing paragraphs.

131. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted, and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant’s duty in this regard.

132. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and comply with applicable industry standards. Defendant’s conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable harm.

133. Defendant’s violations of Section 5 of the FTC Act constitute negligence *per se*.

134. Plaintiff and the Class are within the class of persons that the FTCA is intended to protect.

135. The harm that occurred as a result of the Data Breach is the type of harm the FTCA is intended to guard against. The FTC has pursued enforcement actions against businesses, which, because of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

136. As a direct and proximate result of Defendant’s negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited

to: (i) actual instances of identity theft or fraud; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iv) 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, identity theft; and/or other various forms of fraud (v) costs associated with placing or removing freezes on credit reports; (vi) the continued risk to their PII, which remains 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 its current and former employees and customers in its 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 Plaintiff and the Class.

137. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains 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 in its continued possession.

138. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

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

139. Plaintiff and the Class re-allege and incorporate all foregoing paragraphs.

140. Plaintiff and the Class conferred a monetary benefit to Defendant by providing Defendant with their valuable PII, by permitting Defendant access to their PII so that Defendant could earn revenue by maintaining and utilizing Plaintiff and Class members' PII, which Defendant knowingly used or retained in the course of its business.

141. Defendant benefited from receiving Plaintiff's and the Class members' PII by its ability to retain and use that information for its own financial business benefit. Defendant understood this benefit and accepted the benefit knowingly.

142. Defendant also understood and appreciated that the PII of Plaintiff and the Class was private and confidential to them, and that its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

143. Plaintiff and the Class would not have permitted Defendant to have access to their PII without the implicit promise by Defendant to protect it. Plaintiff

and the Class gave up their privacy to Defendant in exchange for protecting it from others, and Defendant accepted this exchange because it would realize a financial benefit by providing services related to this PII.

144. Instead of providing a reasonable level of security that would have prevented the Data Breach, however, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and the Class by utilizing cheaper, ineffective security measures. Plaintiff and the Class, on the other hand, suffered a direct and proximate result of Defendant's failure to provide the requisite security.

145. But for Defendant's willingness and commitment to maintain privacy and confidentiality, that PII would not have been transferred to and entrusted with Defendant. Indeed, if Defendant had informed its customers that Defendant's data and cyber security measures were inadequate, Defendant would not have been permitted to continue to operate in that fashion.

146. As a result of Defendant's wrongful conduct, Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and the Class. Defendant continues to benefit and profit from their retention and use of the PII while its value to Plaintiff and the Class has been diminished.

147. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this complaint, including compiling, using,

and retaining Plaintiff and the Class's PII, while at the same time failing to maintain that information securely from intrusion and theft by cyber criminals, hackers, and identity thieves.

148. Plaintiff and the Class have no adequate remedy at law.

149. Under principals of equity and good conscience, Defendant should not be permitted to retain the benefits obtained from Plaintiff and the Class because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and the Class were entitled to, and that were mandated by federal, state, and local laws and industry standards.

150. Defendant acquired a monetary benefit and PII through inequitable means, in that they failed to disclose the inadequate security practices previously alleged.

151. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and the Class, proceeds that they unjustly received.

152. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff 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 identify 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 time that the Plaintiff and Class have not been compensated for.

153. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm.

COUNT IV
Declaratory Judgment and Injunctive Relief
(On behalf of Plaintiff and the Class)

154. Plaintiff and the Class re-allege and incorporate all foregoing paragraphs.

155. Plaintiff pursues this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

156. Defendant owes a duty of care to Plaintiff and the Class that require it to adequately secure Plaintiff's and the Class members' PII.

157. Defendant failed to fulfill their duty of care to safeguard Plaintiff's and the Class members' PII.

158. Plaintiff and the Class are at risk of harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

159. Plaintiff, therefore, seeks a declaration that (1) Defendant's existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with their explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

- a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- b. Engaging third-party security auditors and internal personnel to run automated security monitoring;
- c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

- d. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;
- e. Conducting regular database scanning and security checks;
- f. Routinely and continually conducting 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;
- g. Purchasing credit monitoring services for Plaintiff and the Class for a period of ten years; and
- h. Meaningfully educating Plaintiff and the Class 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.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, requests judgment against Defendant and that the Court grant the following:

1. For an order certifying the Class and appointing Plaintiff and his counsel to represent the Class;
2. For an order enjoining Defendant from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of the PII belonging to Plaintiff and the Class;
3. For injunctive relief requiring Defendant to:
 - a. Engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
 - b. Engage third-party security auditors and internal personnel to run automated security monitoring;
 - c. Audit, test, and train its security personnel regarding any new or modified procedures;
 - d. Segment their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

- e. Conduct regular database scanning and security checks;
 - f. 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;
 - g. Purchase credit monitoring services for Plaintiff and the Class for a period of ten years; and
 - h. Meaningfully educate Plaintiff and the Class 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.
- 4. An order instructing Defendant to purchase or provide funds for credit monitoring services for Plaintiff and all Class members;
 - 5. An award of compensatory, statutory, nominal and punitive damages, in an amount to be determined at trial;
 - 6. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
 - 7. An award of reasonable attorney's fees, costs, and litigation expenses, as allowable by law; and

8. Any and all such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands this matter be tried before a jury.

Date: June 18, 2024

Respectfully submitted,

/s/ E. Powell Miller

E. Powell Miller (P39487)

Emily E. Hughes (P68724)

THE MILLER LAW FIRM, P.C.

950 West University Drive

Rochester, MI 48307

Tel: (248) 841-2200

epm@millerlawpc.com

eeh@millerlawpc.com

Gary M. Klinger

MILBERG COLEMAN BRYSON PHILLIPS

GROSSMAN PLLC

227 W. Monroe Street, Suite 2100

Chicago, Illinois 60606

Telephone: 866.252.0878

gklinger@milberg.com

Jeff Ostrow

KOPELOWITZ OSTROW P.A.

One W. Las Olas Blvd., Suite 500

Fort Lauderdale, Florida 33301

Telephone: (954) 525-4100

ostrow@kolawyers.com

Attorneys for Plaintiff and Putative Class