UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION AT CLEVELAND

KENNETH OKONSKI, et al. individually and on behalf of all others similarly situated,

Plaintiffs,

v.

PROGRESSIVE CASUALTY INSURANCE COMPANY,

Defendant.

Case No. 1:23-CV-01548

Hon. Judge Patricia A. Gaughan

CONSOLIDATED CLASS ACTION COMPLAINT
(with Jury Trial Demanded)

Plaintiffs Kenneth Okonski, Bradley Okonski, Edward Reis, Tosif Khan, Kulsoom Tosif, Eduardo Barbosa, Rebecca Johnson, Stephen Johnson, Roxanne Trigg, and Giovanni Madaffari (collectively, "Plaintiffs"), individually and on behalf of all other similarly situated individuals (the "Class" or "Class Members," as defined below), by and through their undersigned counsel, file this Consolidated Class Action Complaint against Progressive Casualty Insurance Company ("Progressive" or "Defendant") and allege the following based on personal knowledge of facts pertaining to them, on information and belief, and based on the investigation of their counsel as to all other matters.

I. NATURE OF THE ACTION

1. This class action seeks to redress Progressive's unlawful, willful, and wanton failure to protect the highly sensitive personally identifiable information ("PII") it collected from approximately 347,100 individuals.[1] Due to Progressive's failure to ensure its third-party call centers maintained adequate data security, procedures, practices, protocols, and user controls, Plaintiffs' and the Class's PII was accessed, viewed, and stolen by unauthorized actors in a massive and preventable data breach (the "Data Breach" or "Breach").[2] As such, Plaintiffs' and the Class's PII is now in the hands of ill-intentioned criminals ***who have already begun to use the PII stolen in the Data Breach for nefarious purposes***.

2. On May 19, 2023, Progressive learned that one of the third-party call centers it negligently hired and negligently failed to supervise (the "call center"), utterly failed to protect the PII of Plaintiffs and the Class from unauthorized access.[3]

3. According to Progressive, on May 19, 2023, Progressive received written notification from one of its call centers that an undisclosed number of the call centers'

---

[1] *See Data Breach Notifications*, OFFICE OF THE MAINE ATTORNEY GENERAL, https://apps.web.maine.gov/online/aeviewer/ME/40/7832b375-dedf-4be0-9437-1329b9c6a55b.shtml (last visited Nov. 14, 2023) (containing a link to a sample of the Notice of Data Breach Letter sent to Plaintiffs and the Class).

[2] *See id.*

[3] *See id.*

employees improperly shared their Progressive access credentials with unauthorized individuals who purportedly performed the employees' call center job duties.[4]

4. Upon information and belief, during the Data Breach, unauthorized individuals acquired the personal and confidential information of some of Progressive's customers, including that of Plaintiffs and the Class.

5. Progressive divulged that the earliest date of employment of any of the involved employees was May 2021, but most were hired during or after the fall of 2022.[5] ***Thus, the Breach occurred for years***.

6. After an investigation, Progressive determined that the following types of highly sensitive information were freely accessible to the unauthorized individuals: first and last names, dates of birth, driver's license numbers, email addresses, phone numbers, financial account numbers, routing numbers, financial institution names, credit/debit card numbers, expiration dates, and Social Security numbers (collectively, the "Private Information").[6]

7. Due to Defendant's negligence and lack of oversight and supervision of the call center, unauthorized individuals obtained everything they need to commit identity theft

---

[4] *Id.*

[5] *Id.*

[6] *See Progressive Casualty Insurance Company*, WASHINGTON STATE OFFICE OF THE ATTORNEY GENERAL, https://www.atg.wa.gov/progressive-casualty-insurance-company (last visited Nov. 14, 2023) (containing a link to a notice letter provided to the Washington State Attorney General's Office).

and fraud and wreak havoc on the financial and personal lives of hundreds of thousands of individuals.

8. Despite Progressive discovering the Data Breach in May 2023, Progressive did not notify Plaintiffs and the Class of the Data Breach until August 1, 2023, via Notice of Security Incident Letters ("Notice Letters").

9. In sum, Plaintiffs and Class Members have had their PII compromised as a result of (i) Progressive's inadequate data security procedures, protocols, and practices; (ii) Progressive's failure to select and utilize third-party vendors with adequate data security, user controls, procedures, practices, and protocols in place; and (iii) Progressive's failure to ensure the third-parties it hired maintained adequate data security, user controls, procedures, practices, and protocols prior to giving them access to Plaintiff's and the Class's PII.

10. Thus, Plaintiffs bring this class action lawsuit on behalf of all persons whose PII was compromised due to Progressive's failure to (i) protect the PII of Plaintiffs and the Class; (ii) ensure the call center it hired adequately protected Plaintiffs' and Class Members' PII prior to giving the call center access to Plaintiffs' and the Class's PII; (iii) select a call center with adequate data security, procedures, practices, infrastructure, user controls, training, and protocols; (iv) investigate the call center's data security measures and user controls prior to hiring the call center to ensure they would adequately protect Plaintiffs' and the Class's PII; (v) supervise the call center's data security measures and user controls during the course of their relationship; (vi) warn Plaintiffs and Class Members of the call center's inadequate information security practices; (vii) ensure the call center

monitored its employees and network for security vulnerabilities and incidents; and (viii) give timely notice of the Data Breach to Plaintiffs and the Class.

11. Defendant betrayed the trust of Plaintiffs and Class Members by failing to properly protect and safeguard their PII, thereby enabling unauthorized individuals to view and steal their valuable and sensitive information.

12. For the rest of their lives, Plaintiffs and Class Members will have to deal with the present and continuing risk of identity thieves possessing and misusing their Private Information. ***Indeed, misuse of the PII stolen in the Data Breach has already occurred.***

13. Plaintiffs and Class Members will have to spend significant time responding to the Breach and are at an immediate, imminent, and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach.

14. Plaintiffs and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their Private Information, loss of privacy, and/or additional damages as described below.

15. Plaintiffs bring this action individually and on behalf of the Class, seeking remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

Plaintiffs

16. Plaintiff **Kenneth Okonski** is domiciled in and a citizen of the State of Illinois. Plaintiff Kenneth Okonski received a Notice of Security Incident letter ("Notice Letter") dated August 1, 2023, from Progressive informing him that his personal information, including his name, address, driver's license number, email address, phone number, and date of birth were compromised in the Data Breach.

17. Plaintiff **Bradley Okonski** is domiciled in and a citizen of the State of Illinois. Plaintiff Bradley Okonski received a Notice Letter dated August 1, 2023, from Progressive informing him that his personal information, including his name, address, driver's license number, email address, phone number, and date of birth were compromised in the Data Breach.

18. Plaintiff **Edward Reis** is domiciled in and a citizen of the State of Connecticut. Plaintiff Reis received a Notice Letter dated August 1, 2023, from Progressive informing him that his personal information, including his name, address, driver's license number, email address, phone number, and date of birth were compromised in the Data Breach.

19. Plaintiff **Tosif Khan** is domiciled in and a citizen of the State of California. Plaintiff Khan received a Notice Letter dated August 1, 2023, from Progressive informing him that his personal information, including his name, address, driver's license number, email address, phone number, and date of birth were compromised in the Data Breach.

20. Plaintiff **Kulsoom Tosif** is domiciled in and a citizen of the State of California. Plaintiff Khan received a Notice Letter dated August 1, 2023, from Progressive informing her that her personal information, including her name, address, driver's license number, email address, phone number, and date of birth were compromised in the Data Breach.

21. Plaintiff **Rebecca Johnson** is domiciled in and a citizen of the State of Texas. Plaintiff Rebecca Johnson received a Notice Letter dated August 1, 2023, from Progressive informing her that her personal information, including her name, address, driver's license number, email address, phone number, and date of birth were compromised in the Data Breach.

22. Plaintiff **Stephen Johnson** is domiciled in and a citizen of the State of Texas. Plaintiff Stephen Johnson received a Notice Letter dated August 1, 2023, from Progressive informing him that his personal information, including his name, address, driver's license number, email address, phone number, and date of birth were compromised in the Data Breach.

23. Plaintiff **Roxanne Trigg** is domiciled in and a citizen of the State of Wisconsin. Plaintiff Roxanne Trigg received a Notice Letter dated August 1, 2023, from Progressive informing her that her personal information, including her name, address, driver's license number, email address, phone number, and date of birth were compromised in the Data Breach.

24. Plaintiff **Giovanni Madaffari** is domiciled in and a citizen of the State of Florida. Plaintiff Giovanni Madaffari received a Notice Letter dated August 1, 2023, from

Progressive informing him that his personal information, including his name, address, driver's license number, email address, phone number, and date of birth were compromised in the Data Breach.

Defendant

25. Defendant **Progressive Casualty Insurance Company** is an Ohio corporation with its principal place of business located at 6300 Wilson Mills Road, Mayfield Village, Ohio, 44143.

III. JURISDICTION AND VENUE

26. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than 100 Class Members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the class are citizens of states different from Defendant.[7]

27. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, it regularly transacts business in this District, and upon

[7] *See Data Security Breach Reports "Progressive Casualty Insurance Company,"* Attorney General of Texas, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (47,786 Texas residents impacted by the Data Breach) (last visited Nov. 14, 2023); *Data Breach Notifications*, OFFICE OF THE MAINE ATTORNEY GENERAL, https://apps.web.maine.gov/online/aeviewer/ME/40/7832b375-dedf-4be0-9437-1329b9c6a55b.shtml (last visited Nov. 14, 2023) (1,730 Maine residents impacted by the Data Breach); *Submitted Breach Notification Sample*, OFFICE OF THE ATTORNEY GENERAL CALIFORNIA DEPARTMENT OF JUSTICE, https://oag.ca.gov/system/files/Experian%20sample%20letter%20California.pdf (last visited Nov. 14, 2023) (indicating California residents were impacted by the Data Breach).

information and belief some Class Members reside in this District.

28. Venue is likewise proper as to Defendant in this District because Defendant's principal place of business is in this District, and a substantial part of the events or omissions giving rise to the claim occurred in this District. 28 U.S.C. § 1391(b)(2).

IV. FACTUAL ALLEGATIONS

A. PROGRESSIVE'S COLLECTION AND DISCLOSURE OF PLAINTIFFS' AND THE CLASS'S PRIVATE INFORMATION.

29. Progressive is an insurance company, based out of Mayfield Village, Ohio,[8] that provides a range of insurance products such as, personal and commercial automobile insurance, motorcycle insurance, boat insurance, property insurance, cyber insurance, and recreational vehicle insurance.[9]

30. In order to obtain products and/or services from Defendant, Progressive required Plaintiffs and the Class to disclose their highly sensitive Private Information to Progressive.

31. After receipt of Plaintiffs' and the Class's confidential Private Information, Progressive disclosed Plaintiffs' and the Class's Private Information to third-party call centers Progressive hired, unbeknownst to Plaintiffs and the Class.

---

[8] *See Progressive Insurance: Campus 1 in Mayfield Village, Ohio,* PROGRESSIVE, https://www.progressive.com/locations/mayfield-village-oh-campus-1/#:~:text=Corporate%20locations%3A%20Campus%201%20in%20Mayfield%20Village%2C%20Ohio%20%7C%20Progressive (last visited Nov. 14, 2023).

[9] *See Explore Products*, PROGRESSIVE, https://www.progressive.com/ (last visited Nov. 14, 2023).

32. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and the Class's Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and the Class's Private Information from unauthorized access and disclosure.

33. These duties did not vanish upon hiring third parties and giving the third-parties access to Plaintiffs' and the Class's Private Information.

34. Progressive had the sole responsibility and duty to ensure that any third parties it hired employed adequate data security, user controls, employee training, and procedures to prevent the unauthorized access and misuse of Plaintiffs' and the Class's Private Information.

35. However, Progressive utterly failed to ensure the call center it hired employed adequate data security, user controls, and employee training prior to allowing it access to Plaintiffs' and the Class's PII, resulting in a massive and preventable data breach.

B. PROGRESSIVE'S MASSIVE AND PREVENTABLE DATA BREACH.

Overview of the Data Breach

36. On May 19, 2023, Progressive was notified that Plaintiffs' and the Class's Private Information, which Progressive was responsible for collecting, safeguarding, and protecting, was accessed by unauthorized individuals in a massive and preventable data breach affecting approximately 347,100 individuals.

37. Progressive inexplicably disclosed the Private Information of Plaintiffs and the Class to a third-party call center who utterly lacked adequate data security, user

controls, and employee data security training and oversight.

38. Thus, from May 2021 through May 2023 unauthorized individuals had unfettered and unauthorized access to Plaintiffs' and the Class's PII to use and abuse as they pleased.

39. Progressive entirely failed to ensure that the call center it selected implemented adequate data security, user controls, and employee data security training prior to disclosing Plaintiffs' and the Class's Private Information to the call center.

40. Due to Progressive's negligence, Plaintiffs and the Class face an imminent risk of identity theft and fraud for the rest of their lives, which is only heightened by the fact that some Plaintiffs and Class Members have already begun to experience misuse of the PII accessed in the Data Breach.

Details of the Data Breach

41. According to Progressive's Notice Letter, on May 19, 2023, Progressive received written notification from one of its third-party call centers regarding an incident involving some of the call center's representatives.[10]

42. The call center's employees improperly shared their Progressive access credentials with unauthorized individuals, who were then able to access the Private Information of Plaintiffs and the Class.[11]

---

[10] *See Data Breach Notifications*, OFFICE OF THE MAINE ATTORNEY GENERAL, https://apps.web.maine.gov/online/aeviewer/ME/40/7832b375-dedf-4be0-9437-1329b9c6a55b.shtml (last visited Nov. 14, 2023).

[11] *Id.*

43. Seeking to hide the severity of the Data Breach, Progressive failed to disclose how many individuals had unauthorized access to the confidential Private Information of Plaintiffs and the Class, but the Notice Letter indicates that it was more than one unauthorized actor.[12]

44. The Data Breach occurred for years, unnoticed and unchecked.

45. "[T]he earliest date of employment for any of the potentially involved employees by the third-party service provider was May 2021, but most were hired during or after the fall of 2022."[13]

46. Progressive offered no information concerning when the unauthorized access stopped or why it went unnoticed and unchecked for such a lengthy period of time. Progressive failed to adequately monitor, audit, or verify the integrity of its vendors' data security practices.

47. The Private Information accessed in the Data Breach included: first and last names, dates of birth, driver's license numbers, email addresses, phone numbers, financial account numbers, routing numbers, financial institution names, credit/debit card numbers, expiration dates, and Social Security numbers.[14]

---

[12] *Id.*

[13] *Id.*

[14] *Id.*

48. Upon information and belief, the unauthorized individuals gained access to Plaintiffs' and the Class's PII to steal it so that they could commit identity theft and fraud and/or sell the stolen PII on the dark web for financial gain.

49. Despite having known about the Data Breach since May 2023, Progressive did not send Notice Letters to victims of the Data Breach until on or around August 1, 2023—months after the Data Breach occurred.[15]

50. Defendant failed to provide timely notice to Plaintiffs and Class Members of the Data Breach.

51. In recognition of the certainly impending risk of future harm Plaintiffs and the Class now face, Progressive made a measly offering of two years of credit monitoring and identity theft protection services to Plaintiffs and the Class. Such an offer is inadequate to protect Plaintiffs and the Class from the lifetime risk of harm they face.

52. Progressive has made no assurances it will cease use of the call center; thus Plaintiffs and the Class remain at a continuing threat of harm.

53. Defendant's actions represent a flagrant disregard of the rights of Plaintiffs and the Class Members, both as to privacy and property.

54. Overall, Defendant failed to take the necessary precautions required to safeguard and protect Plaintiff's and the other Class Members' Private Information from unauthorized access, including failing to supervise, monitor, and oversee all third parties it hired who had access to Plaintiffs' and the Class's PII. Progressive should have ensured

[15] *Id.*

any third parties it hired had adequate data security procedures, practices, and protocols in place to eliminate unauthorized access in the first place.

Progressive has Suffered Prior Data Security Incidents

55. Progressive has repeatedly failed to protect PII in its possession. Indeed, Progressive's lack of adequate data security has been brought to light on more than one occasion.

56. In a strikingly similar data breach in 2006, a Progressive employee wrongfully accessed confidential customer information, including: names, Social Security numbers, dates of birth, and property addresses.[16]

57. "Such incidents underscore the threat posed to corporate data by malicious insiders and by workers who accidentally leak sensitive information[.]"[17]

58. Progressive was aware of the harm that could stem from insider threats and inadequate user controls but chose to turn a blind eye. Had Progressive addressed insider threats more seriously earlier on, it could have prevented this Data Breach from occurring.

59. Progressive's lax data security practices were more recently called into question again in 2015. This time, telematic devices offered by Progressive were noted to

[16] *See* Jaikumar Vijayan, *Data Breach at Progressive Highlights Insider Threat*, COMPUTERWORLD, https://www.computerworld.com/article/2562543/data-breach-at-progressive-highlights-insider-threat.html (last visited Nov. 14, 2023).

[17] *Id.*

have "dozens of security flaws that could be exploited by hackers" that could cause consequences ranging from "data loss to life and limb."[18]

Due to Progressive's recent run of data security flaws, it is evident Progressive does not take data security seriously and does little (if anything) to protect customer data in its possession.

C. PLAINTIFFS' EXPERIENCES.

Plaintiff Kenneth Okonski

60. Plaintiff Kenneth Okonski received a Notice Letter from Progressive informing him that his Private Information, including his name, address, driver's license number, email address, phone number, and date of birth were compromised in the Data Breach.

61. Plaintiff Kenneth Okonski's Private Information was entrusted to Defendant for insurance purposes with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

---

[18] *See Progressive Security Holes Put 2 Million at Risk,* INSURANCE BUSINESS, www.insurancebusinessmag.com/us/news/breaking-news/progressive-security-holes-put-2-million-at-risk-21007.aspx (last visited Nov. 14, 2023) ("Telematics devices offered by Progressive Insurance, called 'Snapshot' dongles, boast dozens of security flaws that could be exploited by hackers. According to Corey Thuen, a security researcher at Digital Bond Labs, Progressive's Snapshot device is perilously insecure and vulnerable to remote cyber attacks that could be dangerous for drivers. Thuen suggested that the insurance giant does 'nothing to encrypt or otherwise protect the information [it] collects,' and as such, 'it would be possible to intercept data passed between the dongles and the insurance providers' servers.'").

62. Plaintiff Kenneth Okonski's Private Information was also entrusted to Defendant with the reasonable expectation and mutual understanding that Progressive would ensure that all third-party vendors it hired implemented adequate data security, procedures, protocols, practices, and user access controls to prevent unauthorized access.

63. Because of the Data Breach, Plaintiff Kenneth Okonski's Private Information is now in the hands of criminals. Plaintiff Kenneth Okonski and all Class Members are now at an imminently impending risk of identity theft and fraud.

64. As a result of the Data Breach, and at Progressive's direction, Plaintiff Kenneth Okonski has already spent at least **12–15 hours** responding to the Data Breach. Among other things, Plaintiff Kenneth Okonski has spent time researching the facts and the scope of the Data Breach, monitoring his accounts and Private Information, reviewing his credit reports, and taking other steps in an attempt to mitigate the adverse consequences of the Data Breach. The letter Plaintiff Kenneth Okonski received from Progressive specifically directed him to take these actions.

65. Plaintiff Kenneth Okonski fears for his personal financial security because, upon information and belief, his PII was accessed, acquired, and stolen by criminals in the Data Breach. Plaintiff Kenneth Okonski has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that the law contemplates and addresses. Plaintiff Kenneth Okonski is a cancer patient who is already under significant emotional and mental stress and anguish. The Data Breach has only made these matters worse.

66. These fears are heightened by the fact that Kenneth Okonski has already suffered actual misuse of his PII. After the Data Breach, Plaintiff Kenneth Okonski experienced fraudulent charges to his financial account. Plaintiff Kenneth Okonski reasonably believes these charges are directly traceable to the Data Breach because Progressive has admitted that some financial information, such as financial account numbers, routing numbers, financial institution names, credit/debit card numbers, and expiration dates, were impacted in the Data Breach.

67. Plaintiff Kenneth Okonski suffered actual injury in the form of damages to and diminution in the value of Plaintiff Kenneth Okonski's PII—a form of intangible property that was compromised as a result of Progressive's Data Breach.

68. Plaintiff Kenneth Okonski has suffered imminent and impending injury arising from the substantially increased risk of fraud and identity theft resulting from his PII being accessed, acquired, and stolen by criminals. This imminent and impending risk of harm is supported by the fact that other Plaintiffs and members of the Class have already experienced misuse of their PII. The fact that Defendants offered Plaintiffs and the Class credit monitoring also confirms the certainly impending risk of identity theft and fraud. Moreover, Plaintiff Kenneth Okonski is at an imminent and impending risk of harm because criminals already have or will post his Private Information on the dark web.

69. Plaintiff Kenneth Okonski has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession and is still being given to third parties with inadequate data security, is protected, and safeguarded from future breaches.

70. Plaintiff Kenneth Okonski has been careful to protect and monitor his identity and does not readily disclose his PII. Had Plaintiff Kenneth Okonski known Progressive would carelessly give his highly sensitive Private Information to third parties with inadequate data security, training, and user controls, he would not have utilized Progressive's services.

71. Plaintiff Kenneth Okonski has suffered an extreme invasion of his privacy because unauthorized individuals had unfettered access to his confidential and personal PII without his knowledge or consent.

72. Plaintiff Kenneth Okonski has suffered a multitude of injuries directly and proximately caused by the Data Breach, including: (i) theft of Plaintiff Kenneth Okonski's valuable PII; (ii) the imminent and certain impending injury flowing from fraud and identity theft posed by Kenneth Okonski's PII being accessed by criminals; (iii) damages to and diminution in value of Plaintiff Kenneth Okonski's PII; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security (and vendors with inadequate data security)—*i.e.*, the difference in value between what Plaintiff Kenneth Okonski should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security, failing to ensure the third-parties it hired maintained adequate data security, and failing to protect Plaintiff Kenneth Okonski's PII; (v) invasion of privacy due to criminals taking possession of his PII and likely posting it on the dark web (if they have not done so already); and (vi) continued risk to Plaintiff Kenneth Okonski's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to

undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

Plaintiff Bradley Okonski

73. Plaintiff Bradley Okonski received a Notice Letter from Progressive informing him that his Private Information, including his name, address, driver's license number, email address, phone number, and date of birth were compromised in the Data Breach.

74. Plaintiff Bradley Okonski's Private Information was entrusted to Defendant for insurance purposes with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

75. Plaintiff Bradley Okonski's Private Information was also entrusted to Defendant with the reasonable expectation and mutual understanding that Progressive would ensure that all third-party vendors it hired implemented adequate data security, procedures, protocols, practices, and user access controls to prevent unauthorized access.

76. Because of the Data Breach, Plaintiff Bradley Okonski's Private Information is now in the hands of criminals. Plaintiff Bradley Okonski and all Class Members are now at an imminently impending risk of identity theft and fraud.

77. As a result of the Data Breach, and at Progressive's direction, Plaintiff Bradley Okonski has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff Bradley Okonski has spent time researching the facts and the scope of the Data Breach, monitoring his accounts and Private Information, reviewing his credit

reports, and taking other steps in an attempt to mitigate the adverse consequences of the Data Breach. The letter Plaintiff Bradley Okonski received from Progressive specifically directed him to take these actions.

78. Plaintiff Bradley Okonski fears for his personal financial security because, upon information and belief, his PII was accessed, acquired, and stolen by criminals in the Data Breach. Plaintiff Bradley Okonski has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that the law contemplates and addresses.

79. Plaintiff Bradley Okonski suffered actual injury in the form of damages to and diminution in the value of Plaintiff Bradley Okonski's PII—a form of intangible property that was compromised as a result of Progressive's Data Breach.

80. Plaintiff Bradley Okonski has suffered imminent and impending injury arising from the substantially increased risk of fraud and identity theft resulting from his PII being accessed, acquired, and stolen by criminals. This imminent and impending risk of harm is supported by the fact that other Plaintiffs and members of the Class have already experienced misuse of their PII. The fact that Defendants offered Plaintiffs and the Class credit monitoring also confirms the certainly impending risk of identity theft and fraud. Moreover, Plaintiff Bradley Okonski is at an imminent and impending risk of harm because criminals already have or will post his Private Information on the dark web.

81. Plaintiff Bradley Okonski has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession and is

still being given to third parties with inadequate data security, is protected, and safeguarded from future breaches.

82. Plaintiff Bradley Okonski has been careful to protect and monitor his identity and does not readily disclose his PII. Had Plaintiff Bradley Okonski known Progressive would carelessly give his highly sensitive Private Information to third parties with inadequate data security, training, and user controls, he would not have utilized Progressive's services.

83. Plaintiff Bradley Okonski has suffered an extreme invasion of his privacy because unauthorized individuals had unfettered access to his confidential and personal PII without his knowledge or consent.

84. Plaintiff Bradley Okonski has suffered a multitude of injuries directly and proximately caused by the Data Breach, including: (i) theft of Plaintiff Bradley Okonski's valuable PII; (ii) the imminent and certain impending injury flowing from fraud and identity theft posed by Bradley Okonski's PII being accessed by criminals; (iii) damages to and diminution in value of Plaintiff Bradley Okonski's PII; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security (and vendors with inadequate data security)—*i.e.*, the difference in value between what Plaintiff Bradley Okonski should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security, failing to ensure the third-parties it hired maintained adequate data security, and failing to protect Plaintiff Bradley Okonski's PII; (v) invasion of privacy due to criminals taking possession of his PII and likely posting it on the dark web (if they have not done so already);

and (vi) continued risk to Plaintiff Bradley Okonski's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

Plaintiff Edward Reis

85. Plaintiff Edward Reis received a Notice Letter from Progressive informing him that his Private Information, including his name, address, driver's license number, email address, phone number, and date of birth were compromised in the Data Breach.

86. Plaintiff Edward Reis's Private Information was entrusted to Defendant for insurance purposes with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

87. Plaintiff Edward Reis's Private Information was also entrusted to Defendant with the reasonable expectation and mutual understanding that Progressive would ensure that all third-party vendors it hired implemented adequate data security, procedures, protocols, practices, and user access controls to prevent unauthorized access.

88. Because of the Data Breach, Plaintiff Edward Reis's Private Information is now in the hands of criminals. Plaintiff Edward Reis and all Class Members are now at an imminently impending risk of identity theft and fraud.

89. As a result of the Data Breach, and at Progressive's direction, Plaintiff Edward Reis has already spent hundreds of hours responding to the Data Breach. Among other things, Plaintiff Edward Reis has spent time researching the facts and the scope of

the Data Breach, monitoring his accounts and Private Information, reviewing his credit reports, addressing fraud and identity theft that has already occurred, and taking other steps in an attempt to mitigate the adverse consequences of the Data Breach. The letter Plaintiff Edward Reis received from Progressive specifically directed him to take these actions.

90. Plaintiff Edward Reis fears for his personal financial security because, upon information and belief, his PII was accessed, acquired, and stolen by criminals in the Data Breach. Plaintiff Edward Reis has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach and the fact that his PII has already been misused. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that the law contemplates and addresses.

91. These fears are heightened by the fact that Edward Reis has already suffered actual misuse of his PII that was exposed in the Data Breach. During and after the Data Breach, Plaintiff Edward Reis experienced the following misuse of his PII:

a) Criminals used his PII to obtain a fraudulent driver's license in his name. Specifically, the criminals used Plaintiff Edward Reis's Private Information to obtain a fake driver's license with his full name, date of birth, driver's license number, and a prior address. This fake driver's license was then used to perpetrate a multitude of crimes.

b) The criminals set up fraudulent accounts under Plaintiff Edward Reis's name with two of the credit bureaus. Criminals used his PII that was exposed in the Data Breach to access his credit report and obtain even more PII.

Additionally, once Plaintiff Edward Reis froze his credit and gained control of the accounts, the criminals continued the impersonation to regain control of the accounts, allowing them to unfreeze his credit so that the identity theft and fraud could continue.

c) Criminals also used his PII to fraudulently purchase automobiles at car dealerships. Specifically, criminals were able to successfully obtain fraudulent financing under Plaintiff Edward Reis's name (and credit) and successfully drive away with two vehicles worth approximately $190,000.00. In the process of obtaining fraudulent financing, the criminals racked up multiple hard inquiries on Plaintiff Edward Reis's credit reports, lowering his credit score. Plaintiff Edward Reis reported the fraud and the identity theft to the police.

d) What is perhaps most concerning is that after the criminals fraudulently purchased the vehicles, ***the criminals fraudulently obtained automobile insurance through none other than Progressive***.

e) Most recently, Plaintiff Edward Reis experienced a fraudulent transaction to his Chase Bank account in October 2023. Plaintiff Edward Reis reasonably believes that someone used his Private Information accessed in the Data Breach to impersonate him to gain access to his financial account at Chase Bank. Reason being, Plaintiff has never lost the debit card associated with this account nor used it online, yet the debit card details were used in a fraudulent online transaction. The Data Breach exposed everything necessary

for someone to assume his identity and gain unauthorized access to the account.

92. Plaintiff Edward Reis suffered actual injury in the form of damages to and diminution in the value of Plaintiff Edward Reis's PII—a form of intangible property that was compromised as a result of Progressive's Data Breach.

93. Plaintiff Edward Reis has suffered imminent and impending injury arising from the substantially increased risk of fraud and identity theft resulting from his PII being accessed, acquired, and stolen by criminals. This imminent and impending risk of harm is supported by the fact that he has already experienced misuse of his PII. The fact that Defendants offered Plaintiffs and the Class credit monitoring also confirms the certainly impending risk of identity theft and fraud. Moreover, Plaintiff Edward Reis is at an imminent and impending risk of harm because criminals already have or will post his Private Information on the dark web.

94. Plaintiff Edward Reis has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession and is still being given to third parties with inadequate data security, is protected, and safeguarded from future breaches.

95. Plaintiff Edward Reis has been careful to protect and monitor his identity and does not readily disclose his PII. To the best of Plaintiff Edward Reis's knowledge, he has never before been the victim of a data breach. Had Plaintiff Edward Reis known Progressive would carelessly give his highly sensitive Private Information to third parties

with inadequate data security, training, and user controls, he would not have utilized Progressive's services.

96. Plaintiff Edward Reis has suffered an extreme invasion of his privacy because unauthorized individuals had unfettered access to his confidential and personal PII without his knowledge or consent.

97. Plaintiff Edward Reis has suffered a multitude of injuries directly and proximately caused by the Data Breach, including: (i) theft and misuse of Plaintiff Edward Reis's valuable PII; (ii) the imminent and certain impending injury flowing from fraud and identity theft posed by Edward Reis's PII being accessed and used by criminals; (iii) damages to and diminution in value of Plaintiff Edward Reis's PII; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security (and vendors with inadequate data security)—*i.e.*, the difference in value between what Plaintiff Edward Reis should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security, failing to ensure the third-parties it hired maintained adequate data security, and failing to protect Plaintiff Edward Reis's PII; (v) invasion of privacy due to criminals taking possession of his PII and misusing it; and (vi) continued risk to Plaintiff Edward Reis's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

Plaintiff Tosif Khan

98. Plaintiff Tosif Khan received a Notice Letter from Progressive informing him that his Private Information, including his name, address, driver's license number, email address, phone number, and date of birth were compromised in the Data Breach.

99. Plaintiff Tosif Khan's Private Information was entrusted to Defendant for insurance purposes with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

100. Plaintiff Tosif Khan's Private Information was also entrusted to Defendant with the reasonable expectation and mutual understanding that Progressive would ensure that all third-party vendors it hired implemented adequate data security, procedures, protocols, practices, and user access controls to prevent unauthorized access.

101. Because of the Data Breach, Plaintiff Tosif Khan's Private Information is now in the hands of criminals. Plaintiff Tosif Khan and all Class Members are now at an imminently impending risk of identity theft and fraud.

102. As a result of the Data Breach, and at Progressive's direction, Plaintiff Tosif Khan has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff Tosif Khan has spent time researching the facts and the scope of the Data Breach, monitoring his accounts and Private Information, reviewing his credit reports, and taking other steps in an attempt to mitigate the adverse consequences of the Data Breach. The letter Plaintiff Tosif Khan received from Progressive specifically directed him to take these actions.

103. Plaintiff Tosif Khan fears for his personal financial security because, upon information and belief, his PII was accessed, acquired, and stolen by criminals in the Data Breach. Plaintiff Tosif Khan has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that the law contemplates and addresses.

104. Plaintiff Tosif Khan suffered actual injury in the form of damages to and diminution in the value of Plaintiff Tosif Khan's PII—a form of intangible property that was compromised as a result of the Data Breach.

105. Plaintiff Tosif Khan has suffered imminent and impending injury arising from the substantially increased risk of fraud and identity theft resulting from his PII being accessed, acquired, and stolen by criminals. This imminent and impending risk of harm is supported by the fact that other Plaintiffs and members of the Class have already experienced misuse of their PII. The fact that Defendant offered Plaintiffs and the Class credit monitoring also confirms the certainly impending risk of identity theft and fraud. Moreover, Plaintiff Tosif Khan is at an imminent and impending risk of harm because criminals already have or will post his Private Information on the dark web.

106. Plaintiff Tosif Khan has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession and is still being given to third parties with inadequate data security, is protected, and safeguarded from future breaches.

107. Plaintiff Tosif Khan has been careful to protect and monitor his identity and does not readily disclose his PII. Had Plaintiff Tosif Khan known Progressive would carelessly give his highly sensitive Private Information to third parties with inadequate data security, training, and user controls, he would not have utilized Progressive's services.

108. Plaintiff Tosif Khan has suffered an extreme invasion of his privacy because unauthorized individuals had unfettered access to his confidential and personal PII without his knowledge or consent.

109. Plaintiff Tosif Khan has suffered a multitude of injuries directly and proximately caused by the Data Breach, including: (i) theft of Plaintiff Tosif Khan's valuable PII; (ii) the imminent and certain impending injury flowing from fraud and identity theft posed by Tosif Khan's PII being accessed by criminals; (iii) damages to and diminution in value of Plaintiff Tosif Khan's PII; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security (and vendors with inadequate data security)—*i.e.*, the difference in value between what Plaintiff Tosif Khan should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security, failing to ensure the third-parties it hired maintained adequate data security, and failing to protect Plaintiff Tosif Khan's PII; (v) invasion of privacy due to criminals taking possession of his PII and likely posting it on the dark web (if they have not done so already); and (vi) continued risk to Plaintiff Tosif Khan's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

Plaintiff Kulsoom Tosif

110. Plaintiff Kulsoom Tosif received a Notice Letter from Progressive informing her that her Private Information, including her name, address, driver's license number, email address, phone number, and date of birth were compromised in the Data Breach.

111. Plaintiff Kulsoom Tosif's Private Information was entrusted to Defendant for insurance purposes with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

112. Plaintiff Kulsoom Tosif's Private Information was also entrusted to Defendant with the reasonable expectation and mutual understanding that Progressive would ensure that all third-party vendors it hired implemented adequate data security, procedures, protocols, practices, and user access controls to prevent unauthorized access.

113. Because of the Data Breach, Plaintiff Kulsoom Tosif's Private Information is now in the hands of criminals. Plaintiff Kulsoom Tosif and all Class Members are now at an imminently impending risk of identity theft and fraud.

114. As a result of the Data Breach, and at Progressive's direction, Plaintiff Kulsoom Tosif has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff Kulsoom Tosif has spent time researching the facts and the scope of the Data Breach, monitoring her accounts and Private Information, addressing the misuse that has already occurred, reviewing her credit reports, and taking other steps in an attempt to mitigate the adverse consequences of the Data Breach. The letter Plaintiff Kulsoom Tosif received from Progressive specifically directed her to take these actions.

115. Plaintiff Kulsoom Tosif fears for her personal financial security because, upon information and belief, her PII was accessed, acquired, and stolen by criminals in the Data Breach. Plaintiff Kulsoom Tosif has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that the law contemplates and addresses.

116. These fears are heightened by the fact that Kulsoom Tosif has already suffered actual misuse of her PII. After the Data Breach, Plaintiff Kulsoom Tosif experienced fraudulent charges to her financial account. Plaintiff Kulsoom Tosif reasonably believes these charges are directly traceable to the Data Breach because Progressive has admitted that some financial information, such as financial account numbers, routing numbers, financial institution names, credit/debit card numbers, expiration dates, were impacted in the Data Breach.

117. Plaintiff Kulsoom Tosif suffered actual injury in the form of damages to and diminution in the value of Plaintiff Kulsoom Tosif's PII—a form of intangible property that was compromised as a result of Progressive's Data Breach.

118. Plaintiff Kulsoom Tosif has suffered imminent and impending injury arising from the substantially increased risk of fraud and identity theft resulting from her PII being accessed, acquired, and stolen by criminals. This imminent and impending risk of harm is supported by the fact that Plaintiff Kulsoom Tosif and other members of the Class have already experienced misuse of their PII. The fact that Defendants offered Plaintiffs and the Class credit monitoring also confirms the certainly impending risk of identity theft and

fraud. Moreover, Plaintiff Kulsoom Tosif is at an imminent and impending risk of harm because criminals already have or will post her Private Information on the dark web.

119. Plaintiff Kulsoom Tosif has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession and is still being given to third parties with inadequate data security, is protected, and safeguarded from future breaches.

120. Plaintiff Kulsoom Tosif has been careful to protect and monitor her identity and does not readily disclose her PII. Had Plaintiff Kulsoom Tosif known Progressive would carelessly give her highly sensitive Private Information to third parties with inadequate data security, training, and user controls, she would not have utilized Progressive's services.

121. Plaintiff Kulsoom Tosif has suffered an extreme invasion of her privacy because unauthorized individuals had unfettered access to her confidential and personal PII without her knowledge or consent.

122. Plaintiff Kulsoom Tosif has suffered a multitude of injuries directly and proximately caused by the Data Breach, including: (i) theft and misuse of Plaintiff Kulsoom Tosif's valuable PII; (ii) the imminent and certain impending injury flowing from fraud and identity theft posed by Kulsoom Tosif's PII being accessed by criminals; (iii) damages to and diminution in value of Plaintiff Kulsoom Tosif's PII; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security (and vendors with inadequate data security)—*i.e.*, the difference in value between what Plaintiff Kulsoom Tosif should have received from Defendant and Defendant's defective and

deficient performance of that obligation by failing to provide reasonable and adequate data security, failing to ensure the third-parties it hired maintained adequate data security, and failing to protect Plaintiff Kulsoom Tosif's PII; (v) invasion of privacy due to criminals taking possession of her PII and likely posting it on the dark web (if they have not done so already); and (vi) continued risk to Plaintiff Kulsoom Tosif's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

Plaintiff Eduardo Barbosa

123. Plaintiff Eduardo Barbosa received a Notice Letter from Progressive informing him that his Private Information, including his name, address, driver's license number, email address, phone number, and date of birth were compromised in the Data Breach.

124. Plaintiff Eduardo Barbosa's Private Information was entrusted to Defendant for insurance purposes with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

125. Plaintiff Eduardo Barbosa's Private Information was also entrusted to Defendant with the reasonable expectation and mutual understanding that Progressive would ensure that all third-party vendors it hired implemented adequate data security, procedures, protocols, practices, and user access controls to prevent unauthorized access.

126. Because of the Data Breach, Plaintiff Eduardo Barbosa's Private Information is now in the hands of criminals. Plaintiff Eduardo Barbosa and all Class Members are now at an imminently impending risk of identity theft and fraud.

127. As a result of the Data Breach, and at Progressive's direction, Plaintiff Eduardo Barbosa has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff Eduardo Barbosa has spent time researching the facts and the scope of the Data Breach, monitoring his accounts and Private Information, reviewing his credit reports, and taking other steps in an attempt to mitigate the adverse consequences of the Data Breach. The letter Plaintiff Eduardo Barbosa received from Progressive specifically directed him to take these actions.

128. Plaintiff Eduardo Barbosa fears for his personal financial security because, upon information and belief, his PII was accessed, acquired, and stolen by criminals in the Data Breach. Plaintiff Eduardo Barbosa has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that the law contemplates and addresses.

129. Plaintiff Eduardo Barbosa suffered actual injury in the form of damages to and diminution in the value of Plaintiff Eduardo Barbosa's PII—a form of intangible property that was compromised as a result of Progressive's Data Breach.

130. Plaintiff Eduardo Barbosa has suffered imminent and impending injury arising from the substantially increased risk of fraud and identity theft resulting from his PII being accessed, acquired, and stolen by criminals. This imminent and impending risk

of harm is supported by the fact that other Plaintiffs and members of the Class have already experienced misuse of their PII. The fact that Defendants offered Plaintiffs and the Class credit monitoring also confirms the certainly impending risk of identity theft and fraud. Moreover, Plaintiff Eduardo Barbosa is at an imminent and impending risk of harm because criminals already have or will post his Private Information on the dark web.

131. Plaintiff Eduardo Barbosa has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession and is still being given to third parties with inadequate data security, is protected, and safeguarded from future breaches.

132. Plaintiff Eduardo Barbosa has been careful to protect and monitor his identity and does not readily disclose his PII. Had Plaintiff Eduardo Barbosa known Progressive would carelessly give his highly sensitive Private Information to third parties with inadequate data security, training, and user controls, he would not have utilized Progressive's services.

133. Plaintiff Eduardo Barbosa has suffered an extreme invasion of his privacy because unauthorized individuals had unfettered access to his confidential and personal PII without his knowledge or consent.

134. Plaintiff Eduardo Barbosa has suffered a multitude of injuries directly and proximately caused by the Data Breach, including: (i) theft of Plaintiff Eduardo Barbosa's valuable PII; (ii) the imminent and certain impending injury flowing from fraud and identity theft posed by Eduardo Barbosa's PII being accessed by criminals; (iii) damages to and diminution in value of Plaintiff Eduardo Barbosa's PII; (iv) loss of the benefit of the

bargain with Defendant to provide adequate and reasonable data security (and vendors with inadequate data security)—*i.e.*, the difference in value between what Plaintiff Eduardo Barbosa should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security, failing to ensure the third-parties it hired maintained adequate data security, and failing to protect Plaintiff Eduardo Barbosa's PII; (v) invasion of privacy due to criminals taking possession of his PII and likely posting it on the dark web (if they have not done so already); and (vi) continued risk to Plaintiff Eduardo Barbosa's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

Plaintiff Rebecca Johnson

135. Plaintiff Rebecca Johnson received a Notice Letter from Progressive informing her that her Private Information, including her name, address, driver's license number, email address, phone number, and date of birth were compromised in the Data Breach.

136. Plaintiff Rebecca Johnson's Private Information was entrusted to Defendant for insurance purposes with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

137. Plaintiff Rebecca Johnson's Private Information was also entrusted to Defendant with the reasonable expectation and mutual understanding that Progressive

would ensure that all third-party vendors it hired implemented adequate data security, procedures, protocols, practices, and user access controls to prevent unauthorized access.

138. Because of the Data Breach, Plaintiff Rebecca Johnson's Private Information is now in the hands of criminals. Plaintiff Rebecca Johnson and all Class Members are now at an imminently impending risk of identity theft and fraud.

139. As a result of the Data Breach, and at Progressive's direction, Plaintiff Rebecca Johnson has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff Rebecca Johnson has spent time researching the facts and the scope of the Data Breach, monitoring her accounts and Private Information, addressing the misuse that has already occurred, reviewing her credit reports, and taking other steps in an attempt to mitigate the adverse consequences of the Data Breach. The letter Plaintiff Rebecca Johnson received from Progressive specifically directed her to take these actions.

140. Plaintiff Rebecca Johnson fears for her personal financial security because, upon information and belief, her PII was accessed, acquired, and stolen by criminals in the Data Breach. Plaintiff Rebecca Johnson has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that the law contemplates and addresses.

141. Plaintiff Rebecca Johnson suffered actual injury in the form of damages to and diminution in the value of Plaintiff Rebecca Johnson's PII—a form of intangible property that was compromised as a result of Progressive's Data Breach.

142. Plaintiff Rebecca Johnson has suffered imminent and impending injury arising from the substantially increased risk of fraud and identity theft resulting from her PII being accessed, acquired, and stolen by criminals. This imminent and impending risk of harm is supported by the fact that other members of the Class have already experienced misuse of their PII. The fact that Defendants offered Plaintiffs and the Class credit monitoring also confirms the certainly impending risk of identity theft and fraud. Moreover, Plaintiff Rebecca Johnson is at an imminent and impending risk of harm because criminals already have or will post her Private Information on the dark web.

143. Plaintiff Rebecca Johnson has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession and is still being given to third parties with inadequate data security, is protected, and safeguarded from future breaches.

144. Plaintiff Rebecca Johnson has been careful to protect and monitor her identity and does not readily disclose her PII. Had Plaintiff Rebecca Johnson known Progressive would carelessly give her highly sensitive Private Information to third parties with inadequate data security, training, and user controls, she would not have utilized Progressive's services.

145. Plaintiff Rebecca Johnson has suffered an extreme invasion of her privacy because unauthorized individuals had unfettered access to her confidential and personal PII without her knowledge or consent.

146. Plaintiff Rebecca Johnson has suffered a multitude of injuries directly and proximately caused by the Data Breach, including: (i) theft and misuse of Plaintiff Rebecca

Johnson's valuable PII; (ii) the imminent and certain impending injury flowing from fraud and identity theft posed by Rebecca Johnson's PII being accessed by criminals; (iii) damages to and diminution in value of Plaintiff Rebecca Johnson's PII; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security (and vendors with inadequate data security)—*i.e.*, the difference in value between what Plaintiff Rebecca Johnson should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security, failing to ensure the third-parties it hired maintained adequate data security, and failing to protect Plaintiff Rebecca Johnson's PII; (v) invasion of privacy due to criminals taking possession of her PII and likely posting it on the dark web (if they have not done so already); and (vi) continued risk to Plaintiff Rebecca Johnson's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

Plaintiff Stephen Johnson

147. Plaintiff Stephen Johnson received a Notice Letter from Progressive informing him that his Private Information, including his name, address, driver's license number, email address, phone number, and date of birth were compromised in the Data Breach.

148. Plaintiff Stephen Johnson's Private Information was entrusted to Defendant for insurance purposes with the reasonable expectation and mutual understanding that

Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

149. Plaintiff Stephen Johnson's Private Information was also entrusted to Defendant with the reasonable expectation and mutual understanding that Progressive would ensure that all third-party vendors it hired implemented adequate data security, procedures, protocols, practices, and user access controls to prevent unauthorized access.

150. Because of the Data Breach, Plaintiff Stephen Johnson's Private Information is now in the hands of criminals. Plaintiff Stephen Johnson and all Class Members are now at an imminently impending risk of identity theft and fraud.

151. As a result of the Data Breach, and at Progressive's direction, Plaintiff Stephen Johnson has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff Stephen Johnson has spent time researching the facts and the scope of the Data Breach, monitoring his accounts and Private Information, reviewing his credit reports, and taking other steps in an attempt to mitigate the adverse consequences of the Data Breach. The letter Plaintiff Stephen Johnson received from Progressive specifically directed him to take these actions.

152. Plaintiff Stephen Johnson fears for his personal financial security because, upon information and belief, his PII was accessed, acquired, and stolen by criminals in the Data Breach. Plaintiff Stephen Johnson has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that the law contemplates and addresses.

153. Plaintiff Stephen Johnson suffered actual injury in the form of damages to and diminution in the value of Plaintiff Stephen Johnson's PII—a form of intangible property that was compromised as a result of Progressive's Data Breach.

154. Plaintiff Stephen Johnson has suffered imminent and impending injury arising from the substantially increased risk of fraud and identity theft resulting from his PII being accessed, acquired, and stolen by criminals. This imminent and impending risk of harm is supported by the fact that other Plaintiffs and members of the Class have already experienced misuse of their PII. The fact that Defendants offered Plaintiffs and the Class credit monitoring also confirms the certainly impending risk of identity theft and fraud. Moreover, Plaintiff Stephen Johnson is at an imminent and impending risk of harm because criminals already have or will post his Private Information on the dark web.

155. Plaintiff Stephen Johnson has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession and is still being given to third parties with inadequate data security, is protected, and safeguarded from future breaches.

156. Plaintiff Stephen Johnson has been careful to protect and monitor his identity and does not readily disclose his PII. Had Plaintiff Stephen Johnson known Progressive would carelessly give his highly sensitive Private Information to third parties with inadequate data security, training, and user controls, he would not have utilized Progressive's services.

157. Plaintiff Stephen Johnson has suffered an extreme invasion of his privacy because unauthorized individuals had unfettered access to his confidential and personal PII without his knowledge or consent.

158. Plaintiff Stephen Johnson has suffered a multitude of injuries directly and proximately caused by the Data Breach, including: (i) theft of Plaintiff Stephen Johnson's valuable PII; (ii) the imminent and certain impending injury flowing from fraud and identity theft posed by Stephen Johnson's PII being accessed by criminals; (iii) damages to and diminution in value of Plaintiff Stephen Johnson's PII; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security (and vendors with inadequate data security)—*i.e.*, the difference in value between what Plaintiff Stephen Johnson should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security, failing to ensure the third-parties it hired maintained adequate data security, and failing to protect Plaintiff Stephen Johnson's PII; (v) invasion of privacy due to criminals taking possession of his PII and likely posting it on the dark web (if they have not done so already); and (vi) continued risk to Plaintiff Stephen Johnson's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

Plaintiff Roxanne Trigg

159. Plaintiff Roxanne Trigg received a Notice Letter from Progressive informing her that her PII, including her name, address, driver's license number, email address, phone number, and date of birth were compromised in the Data Breach.

160. Plaintiff Roxanne Trigg's PII was entrusted to Defendant for insurance purposes with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

161. Plaintiff Roxanne Trigg's PII was also entrusted to Defendant with the reasonable expectation and mutual understanding that Progressive would ensure that all third-party vendors it hired implemented adequate data security, procedures, protocols, practices, and user access controls to prevent unauthorized access.

162. Because of the Data Breach, Plaintiff Roxanne Trigg's PII is now in the hands of criminals. Plaintiff Roxanne Trigg and all Class Members are now at an imminently impending risk of identity theft and fraud.

163. As a result of the Data Breach, and at Progressive's direction, Plaintiff Roxanne Trigg has already spent 15–20 hours responding to the Data Breach and has spent $10–$15 obtaining copies of her credit reports. Among other things, Plaintiff Roxanne Trigg has spent time researching the facts and the scope of the Data Breach, monitoring her accounts and PII, addressing the misuse that has already occurred, reviewing her credit reports, and taking other steps in an attempt to mitigate the adverse consequences of the

Data Breach. The letter Plaintiff Roxanne Trigg received from Progressive specifically directed her to take these actions.

164. Plaintiff Roxanne Trigg fears for her personal financial security because, upon information and belief, her PII was accessed, acquired, and stolen by criminals in the Data Breach. Plaintiff Roxanne Trigg has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that the law contemplates and addresses.

165. Plaintiff Roxanne Trigg suffered actual injury in the form of damages to and diminution in the value of Plaintiff Roxanne Trigg's PII—a form of intangible property that was compromised as a result of Progressive's Data Breach.

166. Plaintiff Roxanne Trigg has suffered imminent and impending injury arising from the substantially increased risk of fraud and identity theft resulting from her PII being accessed, acquired, and stolen by criminals. This imminent and impending risk of harm is supported by the fact that other members of the Class have already experienced misuse of their PII. The fact that Defendants offered Plaintiffs and the Class credit monitoring also confirms the certainly impending risk of identity theft and fraud. Moreover, Plaintiff Roxanne Trigg is at an imminent and impending risk of harm because criminals already have or will post her PII on the dark web.

167. Plaintiff Roxanne Trigg has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession and is

still being given to third parties with inadequate data security, is protected, and safeguarded from future breaches.

168. Plaintiff Roxanne Trigg has been careful to protect and monitor her identity and does not readily disclose her PII. Had Plaintiff Roxanne Trigg known Progressive would carelessly give her highly sensitive PII to third parties with inadequate data security, training, and user controls, she would not have utilized Progressive's services.

169. Plaintiff Roxanne Trigg has suffered an extreme invasion of her privacy because unauthorized individuals had unfettered access to her confidential and personal PII without her knowledge or consent.

170. Plaintiff Roxanne Trigg has suffered a multitude of injuries directly and proximately caused by the Data Breach, including: (i) theft and misuse of Plaintiff Roxanne Trigg's valuable PII; (ii) the imminent and certain impending injury flowing from fraud and identity theft posed by Roxanne Trigg's PII being accessed by criminals; (iii) damages to and diminution in value of Plaintiff Roxanne Trigg's PII; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security (and vendors with inadequate data security)—*i.e.*, the difference in value between what Plaintiff Roxanne Trigg should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security, failing to ensure the third-parties it hired maintained adequate data security, and failing to protect Plaintiff Roxanne Trigg's PII; (v) invasion of privacy due to criminals taking possession of her PII and likely posting it on the dark web (if they have not done so already); and (vi) continued risk to Plaintiff Roxanne Trigg's PII, which remains in the

possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

Plaintiff Giovanni Madaffari

171. Plaintiff Giovanni Madaffari received a Notice Letter from Progressive informing him that his Private Information, including his name, address, driver's license number, email address, phone number, and date of birth were compromised in the Data Breach.

172. Plaintiff Giovanni Madaffari's Private Information was entrusted to Defendant for insurance purposes with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

173. Plaintiff Giovanni Madaffari's Private Information was also entrusted to Defendant with the reasonable expectation and mutual understanding that Progressive would ensure that all third-party vendors it hired implemented adequate data security, procedures, protocols, practices, and user access controls to prevent unauthorized access.

174. Because of the Data Breach, Plaintiff Giovanni Madaffari's Private Information is now in the hands of criminals. Plaintiff Giovanni Madaffari and all Class Members are now at an imminently impending risk of identity theft and fraud.

175. As a result of the Data Breach, and at Progressive's direction, Plaintiff Giovanni Madaffari has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff Giovanni Madaffari has spent time researching the facts and

the scope of the Data Breach, monitoring his accounts and Private Information, reviewing his credit reports, and taking other steps in an attempt to mitigate the adverse consequences of the Data Breach. The letter Plaintiff Giovanni Madaffari received from Progressive specifically directed him to take these actions.

176. Plaintiff Giovanni Madaffari fears for his personal financial security because, upon information and belief, his PII was accessed, acquired, and stolen by criminals in the Data Breach. Plaintiff Giovanni Madaffari has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that the law contemplates and addresses.

177. Plaintiff Giovanni Madaffari suffered actual injury in the form of damages to and diminution in the value of Plaintiff Giovanni Madaffari's PII—a form of intangible property that was compromised as a result of Progressive's Data Breach.

178. Plaintiff Giovanni Madaffari has suffered imminent and impending injury arising from the substantially increased risk of fraud and identity theft resulting from his PII being accessed, acquired, and stolen by criminals. This imminent and impending risk of harm is supported by the fact that other Plaintiffs and members of the Class have already experienced misuse of their PII. The fact that Defendants offered Plaintiffs and the Class credit monitoring also confirms the certainly impending risk of identity theft and fraud. Moreover, Plaintiff Giovanni Madaffari is at an imminent and impending risk of harm because criminals already have or will post his Private Information on the dark web.

179. Plaintiff Giovanni Madaffari has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession and is still being given to third parties with inadequate data security, is protected, and safeguarded from future breaches.

180. Plaintiff Giovanni Madaffari has been careful to protect and monitor his identity and does not readily disclose his PII. Had Plaintiff Giovanni Madaffari known Progressive would carelessly give his highly sensitive Private Information to third parties with inadequate data security, training, and user controls, he would not have utilized Progressive's services.

181. Plaintiff Giovanni Madaffari has suffered an extreme invasion of his privacy because unauthorized individuals had unfettered access to his confidential and personal PII without his knowledge or consent.

182. Plaintiff Giovanni Madaffari has suffered a multitude of injuries directly and proximately caused by the Data Breach, including: (i) theft of Plaintiff Giovanni Madaffari's valuable PII; (ii) the imminent and certain impending injury flowing from fraud and identity theft posed by Giovanni Madaffari's PII being accessed by criminals; (iii) damages to and diminution in value of Plaintiff Giovanni Madaffari's PII; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security (and vendors with inadequate data security)—*i.e.*, the difference in value between what Plaintiff Giovanni Madaffari should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security, failing to ensure the third-parties it hired maintained adequate data

security, and failing to protect Plaintiff Giovanni Madaffari's PII; (v) invasion of privacy due to criminals taking possession of his PII and likely posting it on the dark web (if they have not done so already); and (vi) continued risk to Plaintiff Giovanni Madaffari's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

D. CRIMINALS HAVE USED AND WILL CONTINUE TO USE PLAINTIFFS' PRIVATE INFORMATION TO DEFRAUD THEM.

183. Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach can and will be used in a variety of sordid ways for criminals to exploit Plaintiff and the Class Members and to profit off their misfortune.

184. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[19] For example, with the Private Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other

[19] "Facts + Statistics: Identity Theft and Cybercrime," INSURANCE INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited Nov. 14, 2023) (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

harmful forms of identity theft.[20] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and the Class Members.

The Information Exposed Poses a Substantial Risk of Harm

185. Unfortunately, many bad things can happen if a criminal obtain driver's license numbers, which Progressive already admitted was accessed in the Data Breach at issue.

186. "Fraudsters can use your driver's license number to assume your identity and use it for financial gain. They may open bank accounts, apply for loans or credit cards, make unauthorized purchases, and engage in other forms of fraud using your name and PII."[21]

187. Law enforcement warns there are six common things that can happen if a criminal steals your Driver's License or ID, including:

a) **Criminals can sell driver's licenses on the Dark Web:** "driver's license [are] a valuable asset to people who've had their licenses suspended or revoked due to DUIs or DWIs. One of the most common types of identity theft is the act of selling stolen personal data on the Dark Web. Criminals with outstanding warrants can also buy stolen driver's licenses to assume a

[20] *See, e.g.*, Christine DiGangi, *What Can Someone Do With Your Social Security Number*, CREDIT.COM (Oct. 19, 2023), https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last visited Nov. 14, 2023).

[21] Brian Acton, *Protect Your Identity If Your Driver's License Number is Lost or Stolen*, IDENTITYIQ (July 7, 2023), https://www.identityiq.com/identity-theft/can-a-drivers-license-be-used-for-identity-theft/#:~:text=Fraudsters%20can%20use%20your%20driver's,using%20your%20name%20and%20PII (last visited Nov. 14, 2023).

new identity. You'd be shocked at how low-priced stolen identity information is on the Dark Web. Pilfered driver's license numbers on the Dark Web go for a[s] low as $70."[22]

b) **Criminals can commit driver's license fraud: "**[d]river's license fraud specifically occurs when someone uses counterfeit identity documents or another person's identity to obtain a legitimate driver's license or ID card. This happens when someone is not eligible for a real license. Driver's license fraud is most often committed by an undocumented alien or someone with a suspended or revoked license."[23]

c) **Criminals can create fake IDs using the driver's license number:** "Slightly different from driver's license fraud, criminals only need your driver's license number (not the whole license) to create a fake ID that they can use instead of their own. If they have an outstanding warrant and are detained by law enforcement, a cop will run a background check on your ID (which is probably clean) instead of theirs. When the warrant doesn't show up in the background check, the criminals will evade the arrest. If criminals get stopped for a traffic violation and use your ID, law enforcement will file

[22] Yaniv Masjedi, *Can Someone Steal Your Identity With your ID?*, AURA, https://www.aura.com/learn/can-someone-steal-your-identity-with-your-id (last visited Nov. 14, 2023).

[23] *Id.*

the charges on your driving record, not theirs. So you'll be on the hook for paying traffic tickets and clearing your name in court."[24]

d) **Criminals can create a Synthetic Identity:** "[t]hese "synthetic" identities combine stolen data from data breaches, your real online footprint, and fake information. They may use your real driver's license number with a fake name and date of birth. Then they can establish a synthetic identity to run a phishing scam on social media, open new accounts, obtain government documents, and more. It's nearly impossible to find and stop criminals using a synthetic identity because law enforcement can't determine what's real versus fake."

e) **Criminals can commit identity theft:** "[o]nce identity thieves know your name, address and date of birth, they can plug this information into an online database on the Dark Web, enabling them to steal more data[.]"[25]

f) **Criminals can commit mail fraud:** "[i]f thieves have already stolen your name and address, they can submit a change of address request with the post office and redirect all of your mail, including bank statements, credit cards, checks, your IRS tax return, and more. Your personal information can also be used as security questions to commit bank fraud and hack into your accounts or credit card accounts…Once a fraudster captures enough

[24] *Id.*

[25] *Id.*

> information to piece together your financial life, they can drain your bank accounts, take out loans that they never intend to repay (i.e., loan fraud or reverse mortgage scams), destroy your credit score, and cause long-term financial devastation. Unfortunately, you may never realize this is happening until you're being hounded by debt collection agencies, fail to get approved for a mortgage, or can't get an auto loan due to your negatively affected credit history."[26]

188. "The biggest challenge with driver's license theft is that victims often don't realize that criminals have gained access to their personal information until the damage has been done."[27]

189. Social security numbers are also particularly sensitive pieces of personal information, which were also exposed in the Breach here. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change

[26] *Id.*

[27] Dan Rafter, *What to do if your driver's license is lost, stolen, or exposed in a data breach*, NORTON (June 13, 2023) https://us.norton.com/blog/id-theft/lost-or-stolen-drivers-license (last visited Nov. 14, 2023).

> your Social Security number and it's not a good idea because it is connected to your life in so many ways.[28]
>
> (Emphasis added).

190. Private Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[29]

191. This was a financially motivated Breach, as the only reason the unauthorized individuals would want access to Progressive's customer's information in the first place is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein.

192. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[30] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[31]

---

[28] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last visited Nov. 14, 2023).

[29] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (July 5, 2007), available at https://www.gao.gov/products/gao-07-737.

[30] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, PC (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web (last visited Nov. 14, 2023).

[31] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last visited Nov. 14, 2023).

193. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if criminals get access to Private Information, they ***will*** use it.[32]

194. Criminals may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n 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.[33]

195. For instance, with a stolen social security number, which is part of the Private Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[34]

196. The ramifications of Defendant's failure to keep Class Members' Private Information secure are long lasting and severe. Once that information is stolen, fraudulent

---

[32] Ari Lazarus, *How fast will identity thieves use stolen info?*, MILITARY CONSUMER (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info (last visited Nov. 14, 2023).

[33] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,* GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.

[34] *See, e.g.*, Christine DiGangi, *What Can Someone Do With Your Social Security Number*, CREDIT.COM (Oct. 19, 2023), https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last visited Nov. 14, 2023).

use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

197. Further, criminals often trade stolen Private Information on the "cyber black-market" for years following a breach. Criminals can post stolen Private Information on the internet, thereby making such information publicly available.

198. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened. [35] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names. [36]

199. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future. [37]

200. Defendant's offer of limited identity monitoring to Plaintiffs and the Class is woefully inadequate and will not fully protect Plaintiffs from the damages and harm caused

---

[35] *See Medical ID Theft Checklist*, IDENTITYFORCE, available at https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited Nov. 14, 2023).

[36] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages")*, EXPERIAN, available at https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

[37] *Guide for Assisting Identity Theft Victims,* FEDERAL TRADE COMMISSION (Sept. 2013), available at https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf.

by its failures. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. Once the offered coverage has expired, Plaintiffs and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to Progressive's gross negligence. Furthermore, identity monitoring only alerts someone to the fact that they have *already been the victim of identity theft* (*i.e.*, fraudulent acquisition and use of another person's Private Information)—it does not prevent identity theft.[38] Nor can an identity monitoring service remove personal information from the dark web.[39] "The people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."[40]

201. As a direct and proximate result of the Data Breach, Plaintiffs and the Class have had their Private Information exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of further harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing

[38] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017, 9:00 AM), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (last visited Nov. 14, 2023).

[39] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last visited Nov. 14, 2023).

[40] *Id.*

"freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come. Even more seriously is the identity restoration that Plaintiffs and other Class Members must go through, which can include spending countless hours filing police reports, following Federal Trade Commission checklists, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps.

202. Plaintiffs and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Actual identity theft, including fraudulent credit inquiries and cards being opened in their names;

b. Trespass, damage to, and theft of their personal property including Private Information;

c. Improper disclosure of their Private Information;

d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals and having been already misused;

e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing criminals have their Private Information and that identity thieves have already used that information to defraud other victims of the Data Breach;

f. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of Plaintiffs' and Class Members' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Private Information; and

k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

203. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[41] For example, Private Information can be sold

[41] Anita George, *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 Nov. 14, 2023).

at a price ranging from $40 to $200.[42] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[43]

204. Moreover, Plaintiffs and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant and its call center, is protected from further breaches by the implementation of industry standard security measures, practices, user controls, procedures, and protocols. Defendant has shown itself wholly incapable of protecting Plaintiffs' and the Class's Private Information – especially when considering Progressive's prior data security issues identified above.

205. Plaintiffs and Class Members also have an interest in ensuring that their Private Information that was provided to Progressive's call center is removed from the call center's access.

206. Defendant acknowledged, in the Notice Letter to Plaintiffs and other Class Members, that the Data Breach would cause inconvenience to affected individuals by providing numerous steps for Class Members to take in an attempt to mitigate the harm caused by the Data Breach.

---

[42] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Nov. 14, 2023).

[43] *In the Dark*, VPN OVERVIEW, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Nov. 14, 2023).

207. In particular, the letter acknowledged that financial harm would likely occur, advising Class Members to review and monitoring their free credit reports for suspicious activity.

208. At Progressive's suggestion, Plaintiffs are desperately trying to mitigate the damage Progressive caused them. Given the kind of Private Information Progressive made accessible to third parties who should have never been trusted with it to begin with, Plaintiffs are very likely to incur additional damages.

209. Because identity thieves have their Private Information, Plaintiff and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[44]

210. None of this should have happened because the Data Breach was preventable.

E. DEFENDANT WAS AWARE OF THE RISK OF DATA SECURITY INCIDENTS.

211. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the

[44] *See* Brad Blanchard, *What happens if I change my Social Security number?*, LEXINGTON LAW (Aug. 10, 2022), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html (last visited Nov. 14, 2023).

names of some of the biggest cybersecurity breaches: Target,[45] Yahoo,[46] Marriott International,[47] Chipotle, Chili's, Arby's,[48] and others.[49]

212. Progressive has also experienced more than its fair share of data security issues in recent years.[50]

213. Progressive should certainly have been aware, and indeed was aware, that it was at risk of an internal data breach that could expose the Private Information that it collected and maintained.

214. Progressive was clearly aware of the risks it was taking and the harm that could result from inadequate data security.

---

[45] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/ (last visited Nov. 14, 2023).

[46] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html (last visited Nov. 14, 2023).

[47] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/ (last visited Nov. 14, 2023).

[48] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b (last visited Nov. 14, 2023).

[49] *See, e.g.*, Taylor Armerding, *The 15 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Nov. 8, 2022), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (last visited Nov. 14, 2023).

[50] *See* Jaikumar Vijayan, *Data Breach at Progressive Highlights Insider Threat*, COMPUTERWORLD, https://www.computerworld.com/article/2562543/data-breach-at-progressive-highlights-insider-threat.html (last visited Nov. 14, 2023).

F. PROGRESSIVE COULD HAVE EASILY PREVENTED THE DATA BREACH.

215. Data breaches are preventable.[51] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[52] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[53]

216. "**Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures**. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[54]

217. In a Data Breach like this, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security practices for businesses and their third-party vendors. The FTC guidelines emphasize the importance of

---

[51] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012) (emphasis added).

[52] *Id.* at 17.

[53] *Id.* at 28.

[54] *Id.*(emphasis added).

having a data security plan, regularly assessing risks to computer systems and vendor's computer systems, and implementing safeguards to control such risks.[55]

218. Progressive failed to ensure that the third-party call center it hired maintained industry standard data security procedures, practices, user controls, and protocols necessary to prevent a data breach.

219. Upon information and belief, Progressive failed to ensure its third-party call center met the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

220. Progressive should have used a vendor risk assessment framework, such as NIST SP 800-53, to evaluate the call center's controls, processes, user controls, and policies.

221. To prevent the Data Breach, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless

[55] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf. ; *see also Cybersecurity for Small Business, Vendor Security*, Federal Trade Commission, available at https://www.ftc.gov/system/files/attachments/vendor-security/cybersecurity_sb_vendor-security.pdf.

absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- 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.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[56]

222. In addition, Defendant could and should have implemented, as recommended by the FTC, the following measures for third-party vendors:

- "Include provisions for security in your vendor contracts, like a plan to evaluate and update security controls, since threats change. Make the security provisions that are critical to your company non-negotiable." [57]

- "Establish processes so you can confirm that vendors follow your rules. Don't just take their word for it." [58]

- "Cybersecurity threats change rapidly. Make sure your vendors keep their security up to date." [59]

---

[56] *Id.* at 3–4.

[57] *Cybersecurity for Small Business, Vendor Security*, Federal Trade Commission, available at https://www.ftc.gov/system/files/attachments/vendor-security/cybersecurity_sb_vendor-security.pdf

[58] *Id.*

[59] *Id.*

- "Put controls on databases with sensitive information. Limit access to a need-to-know basis, and only for the amount of time a vendor needs to do a job."[60]

223. Given that Defendant was storing the Private Information of more than 300,000 individuals, Defendant could and should have implemented all of the above measures to prevent the Data breach.

224. Upon information and belief, Progressive failed to do any of the above. Progressive could have easily minimized the trust it gave to the call center within its environment and implemented appropriate user controls. But Progressive utterly failed to do so.

225. Moreover, Defendant could and should have implemented the following precautions to prevent the Data Breach:

- **Pre-Engagement Due Diligence**: "Before hiring a vendor or service provider, run through all of an outsourcing's potential implications for internal operations. This usually entails counsels' review as well as extensive communication between data security staff and all applicable business or operations groups…Examine its policies, procedures, internal controls, and training materials to determine whether it's capable of adapting to constantly

[60] *Id.*

changing data security obligations. Make sure that it's in compliance with all relevant privacy-related laws, regulations, and industry standards." [61]

- **Maintain Oversight**: "Monitoring a vendor's risk potential on an ongoing basis is crucial. Conducting routine vendor oversight can help organizations demonstrate that they acted reasonably, if a data breach or another type of security incident results in regulatory action or litigation. Periodic reviews and assessments of vendor performance are important tools." [62]

226. The Data Breach is prime evidence Progressive did not do its due diligence before selecting the call center as a third-party vendor and did not maintain any level of oversight over the call center, as it should have and as is industry standard.

227. Furthermore, Progressive should have heeded the following warnings and advice when using the third-party call center:

- **Consider Information Security During Vendor Selection:** "When selecting a vendor, you must consider how those vendors handle information security. Talk with your vendors early about their security processes; understand how they handle internal security along with your company's.

[61] *5 steps to help maintain data security in vendor relationships*, LEXOLOGY (Oct. 20, 2022) https://www.lexology.com/library/detail.aspx?g=f565eafd-9b7f-4397-9ecb-32d887703923.

[62] *Id.*

Only sign contracts with those vendors whose internal security processes align with your own security objectives."[63]

- **Audit Third-Party Vendors for Compliance:** "An audit is the only way to see what's really happening with your vendor's security, so perform those audits whenever necessary (say, with particularly high-risk data you're entrusting to a vendor). An audit evaluates how the organization executes against its security compliance framework, as well as its performance in previous audits. Look for indicators of compromise and how well the vendor assesses cybersecurity risk." [64]
- **Require Proof of the Third-Party Vendor's Cybersecurity Programs:** "Proving the third-party vendor has an information security program is only half the battle over third-party breaches. The third-party vendor should be able to demonstrate that it takes risk management seriously and dedicates resources to its vulnerability management program… Ongoing third-party risk monitoring gives you continuous insights into the vendor's cybersecurity program. Hold quarterly reviews to evaluate your vendor's performance metrics and security posture." [65]

---

[63] *How to Prevent Third-Party Vendor Breaches*, RISKOPTICS (Sept. 22, 2023), https://reciprocity.com/blog/how-to-prevent-third-party-vendor-data-breaches/ (last visited Nov. 14, 2023).

[64] *Id.*

[65] *Id.*

- **Adopt a Least-Privileged Model for Data Access:** " Many third-party data breaches have one thing in common: the third party was given more access than necessary to complete its job. Holding third-party service providers to strict least-privileged access management standards will improve your network security significantly. Least-privileged access is the cornerstone of managing vendor risk. A breach will only do minor damage when the third-party vendor's access is restricted to the lowest possible access level." [66]
- **Continuous Monitoring for Third-Party Vendors:** "Third-party vendors play an integral role in your organizational supply chain. They can also introduce multiple risks, including data breaches and compliance violations when not properly monitored. That means evaluating vendors only at the beginning of the business relationship is not enough; you need to monitor your vendors on an ongoing basis. Continuous monitoring assures that the organization remains informed of any changes in the risk profile of its third-party vendors. It also allows you to take new measures and adapt your compliance strategies accordingly. With ongoing monitoring, organizations can detect potential threats earlier and foster a culture of transparency and accountability with their vendors. That, in turn, strengthens the trust and

[66] *Id.*

reliability in the partnership, assuring both parties are aligned in maintaining the highest standards of security and compliance." [67]

228. The foregoing makes it clear that there are generally accepted industry standards Progressive should have followed, but utterly failed to do so, resulting in the Data Breach.

229. In sum, this Data Breach could have easily been prevented.

G. DEFENDANT'S RESPONSE TO THE DATA BREACH WAS INADEQUATE.

230. Defendant failed to inform Plaintiffs and Class Members of the Data Breach in time for them to protect themselves from identity theft.

231. Defendant stated that it discovered the Data Breach in May 2023. And yet, Progressive did not notify affected individuals until August 2023. Even then, Progressive failed to inform Plaintiffs and Class Members exactly what information was exposed, how long it was exposed, and how many individuals had unauthorized access to their Private Information in the Data Breach, leaving Plaintiffs and Class Members unsure as to the seriousness of the Data Breach.

232. If Progressive had actually monitored its third-party vendor, applied appropriate user access controls, and investigated the Data Breach more diligently and reported it sooner, Plaintiffs and the Class could have taken steps to protect themselves sooner and to mitigate the damages caused by the Breach.

[67] *Id.*

V. CLASS ACTION ALLEGATIONS

233. Plaintiffs incorporate by reference all preceding paragraphs as if fully restated here.

234. Plaintiffs bring this action against Progressive on behalf of themselves and on behalf of all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiffs assert all claims on behalf of the following classes, defined as follows:

Nationwide Class (the "Class")

> All individuals residing in the United States who received a Notice Letter from Progressive informing them that their information may have been compromised in the Data Breach.

California Subclass

> All individuals residing in California who received a Notice Letter from Progressive informing them that their information may have been compromised in the Data Breach.

Florida Subclass

> All individuals residing in Florida who received a Notice Letter from Progressive informing them that their information may have been compromised in the Data Breach.

Illinois Subclass

> All individuals residing in Illinois who received a Notice Letter from Progressive informing them that their information may have been compromised in the Data Breach.

235. Excluded from the Classes are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Classes is any judge, justice, or judicial

officer presiding over this matter and members of their immediate families and judicial staff.

236. Plaintiffs reserve the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

237. The proposed Classes meet the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

238. **Numerosity:** The proposed Classes are so numerous that joinder of all members is impracticable. Defendant has reported that the total number of individuals affected in the Data Breach was 347,100 individuals.

239. **Typicality:** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through Progressive's uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class Member because Plaintiffs and each member of the Class had their sensitive Private Information compromised in the same way by the same conduct of Progressive.

240. **Adequacy:** Plaintiffs are adequate representatives of the Class because Plaintiffs' interests do not conflict with the interests of the Class; Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

241. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each

individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress Progressive's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

242. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiffs' and the Class's Private Information;

c. Whether Defendant failed to ensure the third-party vendor it hired had adequate data security, procedures, practices, user controls, and protocols.

d. Whether defendant negligently hired and/or failed to supervise the third-party it hired and gave access to Plaintiffs and the Class's PII;

e. Whether Defendant owed a duty to Plaintiffs and the Class to adequately protect their Private Information, and whether it breached this duty;

f. Whether Progressive breached its duties to Plaintiffs and the Class as a result of the Data Breach;

g. Whether Progressive's conduct, including its failure to act, resulted in or was the proximate cause of the breach;

h. Whether Progressive was negligent in permitting the third-party access to Plaintiffs' and the Class's PII;

i. Whether Progressive was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach;

j. Whether Progressive failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;

k. Whether Progressive continues to breach duties to Plaintiffs and the Class;

l. Whether Plaintiffs and the Class suffered injury as a proximate result of Progressive's negligent actions or failures to act;

m. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief; and

n. Whether Progressive's actions alleged herein constitute gross negligence, and whether Plaintiffs and Class Members are entitled to punitive damages.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

243. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

244. Progressive solicited, gathered, and stored the PII of Plaintiffs and Class Members, which was in turn, provided to a third-party call center Progressive selected.

245. Progressive had full knowledge of the sensitivity of the PII that it possessed and provided to the call center and the potential harm that Plaintiffs and Class Members could and would suffer if their PII were wrongfully accessed by unauthorized individuals.

246. Progressive had a duty to Plaintiffs and Class Members to exercise reasonable care in selecting, monitoring, and ensuring any third-party provider it hired implemented adequate data security, procedures, user controls and protocols to prevent foreseeable harm to Plaintiffs and the Class. Including limiting unnecessary access to Plaintiffs' and the Class's PII.

247. Progressive had a common law duty to exercise reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when selecting a third-party provider. Specifically, when selecting a third-party provider who was entrusted with accessing, storing, safeguarding, handling, collecting, and/or protecting the PII provided by Plaintiffs and the Class.

248. This duty included taking action to ensure that all third-party providers adequately safeguarded such data, limited unnecessary third-party user access to the

Private Information of Plaintiff and the Class, and implemented industry standard security procedures, practices, training, and protocols. Progressive utterly failed to do any of the above.

249. Progressive was also responsible for providing timely notification of the Data Breach to Plaintiff and Class Members but failed to do so, waiting months after the Data Breach to notify victims of the Data Breach.

250. Progressive breached its duties owed to Plaintiffs and the Class by (i) failing to ensure the call center it hired adequately protected Plaintiffs' and Class Members' PII prior to giving the call center access to Plaintiffs' and the Class's PII; (ii) failing to select a call center with adequate data security, procedures, practices, infrastructure, user controls, training, and protocols; (iii) failing to investigate the call center's data security measures and user controls prior to hiring the call center to ensure they would adequately protect Plaintiffs' and the Class's PII; (iv) failing to supervise the call center's data security measures and user controls during the course of their relationship; (v) failing to warn Plaintiffs and Class Members of the call center's inadequate information security practices; (vi) failing to ensure the call center monitored its employees and network for security vulnerabilities and security incidents; (vii) failing give timely notice of the Data Breach to Plaintiffs and the Class; (viii) failing to limit the call center's access to Plaintiffs' and the Class's PII.

251. Plaintiff and the Class were injured as a direct and proximate result of Progressive's breaches of their duties.

252. Plaintiff and Class Members continue to suffer damages and are at an

imminent risk of additional harms and damages due to Progressive's breaches.

253. Accordingly, Plaintiffs and the Class are entitled to compensatory and injunctive relief in an amount to be set forth at trial.

SECOND CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class)

254. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

255. This Count is alleged in the alternative to Plaintiffs' breach of implied contract claim.

256. Plaintiffs and the Class conferred a monetary benefit on Defendant by paying money for insurance services, a portion of which was intended to have been used by Progressive to ensure that any vendors it hired implemented appropriate data security measures and implemented appropriate user controls. Plaintiffs and Class Members further conferred a benefit on Progressive by entrusting their Private Information to it and from which Progressive derived profits.

257. Defendant collected, maintained, and stored the Private Information of Plaintiff and Class Members and, as such, Defendant had direct knowledge of the monetary benefits conferred upon it by Plaintiffs and Class Members.

258. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiffs and Class Members and accepted that monetary benefit.

259. However, acceptance of the benefit under the facts and circumstances described herein make it inequitable for Defendant to retain that benefit without payment

of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on a third-party with adequate data security measures, procedures and protocols to secure Plaintiffs' and Class Members' Private Information. Instead of paying for a third-party who provided a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing a cheaper third-party with little to no data security measures in place. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

260. Under the principle of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiffs and Class Members because Defendant failed to ensure any third-party it hired implemented the appropriate data management and security measures.

261. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices of the third-party it retained, who had access to Plaintiffs' and the Class's PII.

262. If Plaintiffs and Class Members knew that Defendant had given their Private Information to a third-party with virtually no data security measures in place, they would not have agreed to allow Defendant to have or maintain their Private Information.

263. Plaintiffs and Class Members have no adequate remedy at law.

264. As a direct and proximate result of Defendant's decision to profit rather than hire a third-party with adequate data security measures in place, Plaintiffs and Class

Members suffered and continue to suffer actual damages, including (i) the amount of the savings and costs Defendant reasonably should have expended to provide a third-party with adequate data security measures to secure Plaintiffs' Private Information, (ii) time and expenses mitigating harms, (iii) diminished value of the Private Information, (iv) harms as a result of identity theft; and (v) an increased risk of future identity theft.

265. Defendant, upon information and belief, has therefore engaged in opportunistic, unethical, and immoral conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiffs and the Class in direct violation of Plaintiffs' and Class Members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its wrongful conduct.

266. Accordingly, Plaintiffs and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiffs and the Class.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

267. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

268. Defendant required Plaintiffs and Class Members to provide their Private Information to Progressive in order for Progressive to provide services. In exchange, Defendant entered into implied contracts with Plaintiffs and Class Members in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiffs'

and Class Members' Private Information and to timely notify them in the event of a data breach.

269. Plaintiffs and Class Members would not have provided their Private Information to Defendant had they known that Defendant would not safeguard their Private Information, as promised, or provide timely notice of a data breach.

270. Plaintiffs and Class Members would not have provided their Private Information to Defendant had they known that Defendant would hand it over to a third-party with no data security measures in place and would not implement appropriate user controls to protect their PII.

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

272. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' Private Information by carelessly giving it to a third-party with inadequate data security measures, procedures, and protocols, failing to implement user controls, and by failing to provide them with timely and accurate notice of the Data Breach.

273. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class Members.

FOURTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Nationwide Class)

274. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

275. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

276. Defendant owes duties of care to Plaintiffs and Class Members that require Defendant to adequately secure their Private Information and ensure it is not given to third parties with inadequate data security measures.

277. Defendant still possesses Plaintiffs' and Class Members' Private Information and is still giving their PII to third parties with inadequate data security and user controls.

278. Defendant does not specify in the Notice Letters what specific steps it has taken to prevent a data breach from occurring again. Nor has it stated it terminated its relationship with the call center.

279. Plaintiffs and Class Members are at risk of harm due to the exposure of their Private Information and Defendant's failure to address the security failings that lead to such exposure.

280. Plaintiffs, therefore, seek a declaration that (i) Defendant's existing security measures, procedures, user controls, and protocols do not comply with its duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (ii) to comply with its duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a) Monitoring and overseeing all third-parties it hires.

b) Ensuring all third-parties it hires employ industry standard data security measures, procedures, practices, user controls, and protocols.

c) Engaging third-party security auditors and internal personnel to run automated security monitoring;

d) Auditing, testing, and training their security personnel and third-parties regarding any new or modified procedures;

e) Segmenting their user applications by, among other things, creating access controls;

f) Conducting regular database scanning and security checks;

g) Routinely and continually conducting internal training and education to inform internal security personnel and third-parties how to identify and contain a breach when it occurs and what to do in response to a breach;

h) Purchasing credit monitoring services for Plaintiffs and Class Members for a period of ten years; and

i) Meaningfully educating Plaintiffs and Class Members about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps they must take to protect themselves.

FIFTH CAUSE OF ACTION
NEGLIGENT TRAINING, HIRING, AND SUPERVISION
(On behalf of Plaintiffs and the Nationwide Class)

281. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

282. At all relevant times, the call center was Progressive's agent. Progressive granted the call center access to the PII of Plaintiffs and the Class without properly vetting

the third-party, inquiring about/ investigating the third-party's data security, training the third-party, advising the third-party of its duties owed to Plaintiffs and the Class, and/or advising the third-party of the confidential nature of Plaintiffs' and the Class's PII.

283. Progressive was negligent and failed to exercise the requisite standard of care in the hiring, supervision, and retention of the call center, who disclosed Plaintiffs' and the Class's PII without authorization and caused the damages delineated herein by virtue of the Data Breach.

284. At all times relevant hereto, Progressive owed a duty to Plaintiffs and the Class to train and supervise its agents and third parties handling sensitive PII in its possession to ensure they recognized the duties owed to Plaintiffs' and the Class to keep their PII safe from unauthorized access.

285. Progressive owed a duty to Plaintiffs and the Class to ensure the call center implemented adequate data security, procedures, user controls, and protocols sufficient to protect Plaintiffs' and the Class's PII from unauthorized access prior to hiring the call center.

286. Progressive also owed a continuing duty to Plaintiffs and the Class to ensure the call center continued to employ adequate data security, procedures, user controls, and protocols sufficient to protect Plaintiffs' and the Class's PII from unauthorized access after hiring the third-party.

287. Progressive breached this duty by failing to ensure the third-party possessed the requisite data security, procedures, practices, user controls, infrastructure, and

protocols to protect Plaintiffs' and the Class's PII from unauthorized access prior to hiring the third-party and while the third-party worked for Progressive.

288. Progressive was on notice of the importance of data security because of well publicized data breaches occurring throughout the United States, and the prior insider threat Progressive has already dealt with. Despite knowledge of prior data breaches and unauthorized access, Progressive failed to ensure the third-party possessed the adequate security posture to protect Plaintiffs' and the Class's PII from unauthorized disclosure.

289. Progressive knew or should have known that the failure to ensure the third-party employed adequate data security, procedures, user controls, and protocols would create an unreasonable risk of danger to persons and property.

290. As a direct and proximate result of Progressive's breach of its duties, and its negligent hiring, training, selection, and supervision, of the third-party, which resulted in the unauthorized access of Plaintiffs' and Class Members' confidential PII, Plaintiffs and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, diminution in value of their PII, and actual misuse of their PII.

291. Progressive was advised of the Breach, but continues to employ the third-party, putting Plaintiff and the Class at risk of more data breaches in the future.

292. The acts and omissions of Progressive in negligently hiring, retaining, training, and/or supervising the third-party are such as to show gross negligence and reckless disregard for the safety of others and, therefore, punitive damages are appropriate.

SIXTH CAUSE OF ACTION
VIOLATIONS OF CALIFORNIA'S CONSUMER PRIVACY ACT,
CAL. CIV. CODE § 1798.100, *ET SEQ.* ("CCPA")
(On behalf of Plaintiffs Tosif Khan and Kulsoom Tosif and the California Subclass)

293. Plaintiffs Tosif Khan and Kulsoom Tosif incorporate the foregoing paragraphs as though fully set forth herein.

294. Plaintiffs Tosif Khan and Kulsoom Tosif ("Plaintiffs" for the purposes of this Count) bring this Count on their own behalf and on behalf of the California Subclass.

295. The California Legislature has explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[68]

296. The CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

297. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information

[68] California Consumer Privacy Act (CCPA) Compliance, https://buyergenomics.com/ccpa-complience/.

from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(c). Progressive failed to adhere to this directive.

298. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

299. Plaintiffs and California Subclass Members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

300. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

a) is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b) "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c) does business in California; and

d) has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

301. The Private Information taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A).

302. Plaintiffs' and California Subclass Members' unencrypted and unredacted Private Information was subject to unauthorized access and exfiltration, theft, or disclosure because their PII, including name and contact information was wrongfully taken, accessed, and viewed by unauthorized individuals.

303. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures, user controls, and practices appropriate to the nature of the information to protect Plaintiffs' and California Subclass Members' PII.

304. The Data Breach also occurred as a result of Defendant's failure to require by contract that the call center implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use modification or disclosure.

305. At this time, Plaintiffs and California Class Members seek only actual pecuniary damages suffered as a result of Defendant's violations of the CCPA, injunctive

and declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and any other relief the court deems proper.

306. On or about October 25, 2023, Plaintiffs provided written notice to Defendant identifying the specific provisions of this title they allege it has violated. If within 30 days of Plaintiffs' written notice to Defendant it fails to "actually cure" its violations of Cal. Civ. Code § 1798.150(a) and provide "an express written statement that the violations have been cured and that no further violations shall occur," Plaintiffs will amend this complaint to also seek the greater of statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident, or actual damages, whichever is greater. See Cal. Civ. Code § 1798.150(b).

307. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices and as a result of Defendant's failure to ensure its vendor implemented and maintained reasonable security procedures and practices that resulted in the Data Breach, Plaintiffs seek injunctive relief, including public injunctive relief, declaratory relief, and any other relief as deemed appropriate by the Court.

SEVENTH CAUSE OF ACTION
VIOLATIONS OF THE CALIFORNIA CUSTOMER RECORDS ACT
Cal. Civ. Code §§ 1798.80, *et seq*.
(On behalf of Plaintiffs Tosif Khan and Kulsoom Tosif and the California Subclass)

308. Plaintiffs Tosif Khan and Kulsoom Tosif incorporate the foregoing paragraphs as though fully set forth herein.

309. Plaintiffs Tosif Khan and Kulsoom Tosif ("Plaintiffs" for the purposes of this Count) bring this Count on their own behalf and on behalf of the California Subclass.

310. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

311. Defendant is a business that owns, maintains, and licenses Personal Information, within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiffs and California Subclass Members.

312. Businesses that own or license computerized data that includes Personal Information are required to notify California residents when their Personal Information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82.

313. Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

314. Defendant is a business that owns or licenses computerized data that includes Personal Information as defined by Cal. Civ. Code § 1798.82.

315. Plaintiffs and California Subclass Members' Personal Information includes Personal Information as covered by Cal. Civ. Code § 1798.82.

316. Because Defendant reasonably believed that Plaintiffs' and California Subclass Members' Personal Information was acquired by unauthorized persons during the Data Breach, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

317. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Cal. Civ. Code § 1798.82.

318. As a direct and proximate result of Defendant's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiffs and California Subclass Members suffered damages, as described above.

319. Plaintiffs and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

EIGHTH CAUSE OF ACTION
VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW
CAL. BUS. & PROF. CODE § 17200, *ET SEQ.*
(On behalf of Plaintiffs Tosif Khan and Kulsoom Tosif and the California Subclass)

320. Plaintiffs Tosif Khan and Kulsoom Tosif incorporate the foregoing paragraphs as though fully set forth herein.

321. Plaintiffs Tosif Khan and Kulsoom Tosif ("Plaintiffs" for the purposes of this Count) bring this Count on their own behalf and on behalf of the California Subclass.

322. The UCL prohibits any "unlawful" or "unfair" business act or practice, as those terms are defined by the UCL and relevant case law. By virtue of the above-described

wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful and unfair practices within the meaning, and in violation, of the UCL.

323. In the course of conducting its business, Defendant committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and California Subclass Members' Private Information, failing to ensure its vendors did the same, and by violating the statutory and common law alleged herein, including, *inter alia*, the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100, *et seq.*), Article I, Section 1 of the California Constitution (California's constitutional right to privacy), Cal. Civil Code § 1798.81.5, 45 C.F.R. § 164, *et seq.*, and Section 5 of the FTC Act.

324. Plaintiffs and California Subclass Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

325. Defendant also violated the UCL by failing to timely notify Plaintiffs and California subclass Members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their Private Information. If Plaintiffs and California Subclass Members had been notified in an appropriate fashion, they could have taken precautions to safeguard and protect their Private Information and identities.

326. Defendant violated the unfair prong of the UCL by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and California Subclass Members' Private Information with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and California Subclass Members' Private Information in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Subclass Members. They were likely to deceive the public into believing their Private Information was securely stored when it was not. The harm these practices caused to Plaintiffs and California Subclass Members outweighed their utility, if any.

327. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendant's wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendant's practices are also contrary to legislatively declared and public policies that seek to protect Private Information and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA and the FTC Act (15 U.S.C. § 45). The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

328. Plaintiffs and California Subclass Members suffered injury in fact and lost money or property as a result of Defendant's violations of statutory and common law. Plaintiffs and the California Subclass suffered from overpaying for services that should have included adequate data security for their Private Information, by experiencing a diminution of value in their Private Information as a result if its theft by cybercriminals, the loss of Plaintiffs' and California Subclass Members' legally protected interest in the confidentiality and privacy of their Private Information, and additional losses as described above.

329. Plaintiffs and California Subclass Members have also suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) deprivation of the value of their PII for which there is a well-established national and international market, and/or (v) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

330. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. As such, Plaintiffs, on behalf of themselves and California Subclass Members, seeks restitution and an injunction, including public injunctive relief prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data

security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the Private Information entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203. To the extent any of these remedies are equitable, Plaintiffs and the Class seek them in the alternative to any adequate remedy at law they may have.

NINTH CAUSE OF ACTION
VIOLATION OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT ("FDUTPA"), FLA. STAT. § 501.201 *ET SEQ.*
(On Behalf of Plaintiff Giovanni Madaffari and the Florida Subclass)

331. Plaintiff Giovanni Madaffari incorporates the foregoing paragraphs as though fully set forth herein.

332. Plaintiff Giovanni Madaffari ("Plaintiff" for the purposes of this Count) brings this Count on his own behalf and on behalf of the Florida Subclass (the "Class" for purposes of this Count").

333. FDUTPA prohibits "unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." Fla. Stat.§ 501.204.

334. Defendant engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce.

335. While engaged in trade or commerce, Defendant violated FDUTPA, including, among other things, by:

a) Failing to implement and maintain appropriate and reasonable security procedures and practices to safeguard and protect the Private Information of Plaintiff and the Class from unauthorized access and disclosure;

b) Failing to disclose that its third-party's computer systems and data security practices were inadequate to safeguard and protect the Private Information of Plaintiff and the Class from being compromised, stolen, lost, or misused; and

336. Defendant knew or should have known that their computer systems and data security practices and their vendor's data security practices were inadequate to safeguard Class Members' Private Information entrusted to it, and that risk of a data breach or theft was highly likely.

337. Defendant should have disclosed this information because they were in a superior position to know the true facts related to the defective data security. Indeed, Defendant was solely responsible for selecting the vendors it employed and Plaintiff and the Class had no input.

338. Defendant's failures constitute false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and Class Members) regarding the security of Plaintiff's and the Class's Private Information.

339. The representations upon which impacted individuals (including Plaintiff and Class Members) relied were material representations (*e.g.*, as to Defendant' adequate protection of Private Information), and consumers (including Plaintiff and Class Members)

relied on those representations to their detriment.

340. Defendant's actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Defendant engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to Plaintiff and the Class.

341. In committing the acts alleged above, Defendant engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to Plaintiff and the Class that it did not follow industry best practices for the collection, use, and storage of Private Information and the selection of vendors.

342. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiff's and Class Members' Private Information was disclosed to third parties without authorization, causing and will continue to cause Plaintiff and Class Members damages. Accordingly, Plaintiff and Class Members are entitled to recover an order providing declaratory and injunctive relief and reasonable attorneys' fees and costs, to the extent permitted by law.

343. Also, as a direct result of Defendant's knowing violation of the Florida Deceptive and Unfair Trade Practices Act, Plaintiff and Class Members are entitled to injunctive relief, including, but not limited to:

a) Ordering Defendant to ensure that all third-party vendors it engages employ adequate data security, training, user controls, and protocols prior to releasing Plaintiffs' and the Class's Private Information.

b) Requiring Defendant to thoroughly and regularly evaluate any vendor's or third-party's technology that allows or could allow access to Private Information and to promptly migrate to superior or more secure alternatives.

TENTH CAUSE OF ACTION
VIOLATIONS OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT ("CFA"), 815 ILL. COMP. STAT. §§ 505/1, *ET SEQ.*
(On Behalf of Plaintiffs Bradley Okonski and Kenneth Okonski and the Illinois Subclass)

344. Plaintiffs Bradley Okonski and Kenneth Okonski incorporate the foregoing paragraphs as though fully set forth herein.

345. Plaintiffs Bradley Okonski and Kenneth Okonski ("Plaintiffs" for the purposes of this Count) bring this Count on his own behalf and on behalf of the Illinois Subclass.

346. Plaintiffs and the Class are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiffs, the Class, and Defendant are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

347. Defendant engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engages in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

348. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the CFA, including: (i) failing

to keep Plaintiffs' and the Class Members' sensitive PII from being unlawfully accessed; (ii) failing to ensure the vendors and third-parties it hired maintained adequate data security, training, user controls, and protocols; (iii) failing to disclose or omitting material facts to Plaintiffs and the Class regarding their vendor's lack of adequate data security and inability or unwillingness to properly secure and protect the PII of Plaintiffs and the Class; (iii) failing to disclose or omitting materials facts to Plaintiffs and the Class about Defendant's and its vendors failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII of Plaintiffs and the Class; and (iv) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs' and the Class's PII and other PII from further unauthorized disclosure, release, data breaches, and theft.

349. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about their vendor's inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiffs and the Class and defeat their reasonable expectations about the security of their PII.

350. Defendant intended that Plaintiffs and the Class rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

351. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Class. Plaintiffs and the Class have been adversely affected by Defendant's conduct and

the public was and is at risk as a result thereof.

352. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiffs and the Class of the nature and extent of the Data Breach pursuant to the Illinois PII Protection Act, 815 ILCS 530/1, *et seq*.

353. As a result of Defendant's wrongful conduct, Plaintiffs and the Class were injured in that they never would have provided their PII to Defendant, or purchased Defendant's services, had they known or been told that Defendant would provide their PII to vendors with insufficient data security measures in place.

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

355. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiffs and the Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the CFA.

ELEVENTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On behalf of the Plaintiffs and the Nationwide Class)

356. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

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

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

359. Because of the highly sensitive nature of the PII, Plaintiffs and Class members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices and its failure to select third-party vendors with adequate data security procedures, protocols, and user access controls.

360. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to protect Plaintiffs' and Class members' PII by relinquishing it to a third-party vendor with inadequate data security procedures and protocols in place.

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

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

TWELFTH CAUSE OF ACTION
INVASION OF PRIVACY
(INTRUSION UPON SECLUSION)
(On behalf of Plaintiffs and the Nationwide Class)

363. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

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

365. As a result of Defendant's conduct, publicity was given to the Private Information of the Plaintiffs and Class Members which necessarily includes matters concerning their private life such as their PII.

366. The Private Information of the Plaintiffs and Class Members is not of legitimate public concern and should remain private.

367. By knowingly failing to keep the Private Information of the Plaintiffs and Class Members safe, and by knowingly misusing said information, Defendant negligently, recklessly, and intentionally invaded privacy of the Plaintiff and Class Member by intruding into the private affairs of the Plaintiff and Class Members, without approval, in a manner that would be highly offensive and objectionable to a person of ordinary sensibilities.

368. Defendant knew that an ordinary person in the position of the Plaintiffs or Class Members would consider Defendant's negligent, reckless, and intentional actions highly offensive and objectionable.

369. Such an intrusion into the private affairs of the Plaintiffs and Class Members is likely to cause outrage, shame, and mental suffering because the Private Information disclosed includes financial information and sensitive personal information like Social Security Numbers that allow third parties to commit fraud and identity theft.

370. Defendant invaded the right to privacy of the Plaintiffs and the Class Members and intruded into the private lives of the Plaintiffs and Class members by negligently, recklessly, and intentionally misusing their Private Information without their informed, voluntary, affirmative, and clear consent.

371. Defendant intentionally concealed from Plaintiffs and Class Members an incident that misused their Private information without their informed, voluntary, affirmative, and clear consent.

372. As a proximate result of such intentional misuse, the reasonable expectations of privacy that the Plaintiffs and Class Members have in their Private Information was unduly frustrated and thwarted.

373. Defendant's conduct, amounting to a substantial and serious invasion of the protected privacy concerns of the Plaintiffs and Class Members causing anguish and suffering such that a person with ordinary sensibilities would consider Defendant's intentional actions or inaction highly offensive and objectionable.

374. In failing to protect Plaintiffs' and Class Members' Private Information, and in negligently, recklessly, and intentionally misusing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of the rights of the Plaintiff and Class Members to have such information kept secure, confidential, and private.

375. As a direct and proximate result of Defendant's invasion of privacy, the Plaintiffs and Class Members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in the

possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information of the Plaintiff and Class Members.

376. The Plaintiffs and Class Members are entitled to compensatory, consequential, punitive, and nominal damages suffered as a result of the Data Breach.

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

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

a) An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Classes as requested herein, appointing the undersigned as counsel for the Classes, and finding that Plaintiffs are proper representatives of the Classes requested herein;

b) A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c) An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d) An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e) A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f) An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all appropriate issues raised in this Consolidated Complaint.

Dated: November 20, 2023

Respectfully submitted,

/s/:William B. Federman

William B. Federman
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
wbf@federmanlaw.com

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN LLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Interim Co-Lead Class Counsel for Plaintiffs and the Putative Class

Brian D. Flick, Esq (OH 0081605)
DannLaw
15000 Madison Avenue
Lakewood, OH 44107
(513) 645-3488
(216) 373-0536 facsimile
notices@dannlaw.com

Interim Liaison Class Counsel for Plaintiffs and the Class