UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION AT DAYTON

In Re Motility Data Breach Litigation	Case No. 3:25-cv-00330 Honorable Walter H. Rice **DEMAND FOR JURY TRIAL**

CONSOLIDATED CLASS ACTION COMPLAINT

G. Scott Lockwood, Heather Reynicke, Christopher Santora, Donna Mathews, John Langan, Nancy Langan, Stephen Duesler, Patrick Hubley, and Peggy L. Koller ("Plaintiffs"), through their attorneys, on behalf of themselves and all others similarly situated, bring this Consolidated Class Action Complaint against Motility Software Solutions, Inc. ("Motility" or "Defendant"), alleging as follows upon information and belief, investigation of counsel, and personal knowledge of Plaintiffs:

INTRODUCTION

1. This class action arises from Defendant's failure to protect highly sensitive data.

2. On August 19, 2025, Motility discovered it had lost control over its computer network and cybercriminals accessed, copied and removed the highly sensitive personal information of its clients and their customers.

3. On or around September 12, 2025, Motility's parent company, The Reynolds and Reynolds Company, disclosed Motility's Data Breach.[1]

4. It is unknown how long the data breach continued before Motility identified

[1] *Motility Software Solutions Discloses Data Security Incident*, Reynolds & Reynolds (Sept. 12, 2025), https://www.reyrey.com/company/media-center/news-releases/motility-software-solutions-discloses-data-security-incident (last visited Nov. 4, 2025).

"suspicious activity" on August 19, 2025. Indeed, Defendant reported to multiple state attorneys general that the Data Breach began on August 11, 2025, suggesting that cybercriminals had unfettered access to Plaintiffs' and the Class's PII for at least *eight days*.[2]

5. According to the Data Breach Notification Defendant provided to the Office of the Maine Attorney General, the Data Breach affected 766,670 consumers.[3]

6. And yet, Defendant waited until September 29, 2025, over a month after it discovered the Data Breach, before it began directly notifying Plaintiffs and the Class (the "Breach Notice"). A sample breach notice Defendant sent to Plaintiff Mathews and to the California Attorney General's Office[4] are collectively attached to hereto as **Exhibit A**.

7. Upon information and belief, cybercriminals were able to breach Defendant's systems over an undisclosed period of time because Defendant failed to adequately train its employees on cybersecurity, failed to adequately monitor its agents, contractors, vendors, and suppliers in handling and securing the private information of Plaintiffs, and failed to maintain reasonable security safeguards or protocols to protect the Class's private information—rendering it an easy target for cybercriminals.

8. Reynolds and Reynolds Company's notice of the Motility Data Breach and Defendant's Breach Notice intentionally obfuscate the nature of the Data Breach and the threat it poses. The notices do not disclose how the Data Breach happened, who perpetrated the breach,

---

[2] *See, e.g. Motility Software Solutions Inc*, Wash. State Off. of the Att'y Gen., https://www.atg.wa.gov/motility-software-solutions-inc (last visited Nov. 4, 2025); *Data Breach Notifications: Motility Software Solutions, Inc*, Office of the Me. Att'y Gen., https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/f23710aa-efa8-4dff-b698-bc94ae180af8.html (last visited Nov. 4, 2025).

[3] *Data Breach Notifications*, Office of the Me. Att'y Gen, *supra*, n.2.

[4] *See Submitted Breach Notification Sample*, Office of the Att'y Gen., Cal. Dep't of Justice, https://oag.ca.gov/ecrime/databreach/reports/sb24-610795 (last visited Nov. 4, 2025).

whether a ransom was demanded or paid, how long the breach lasted, or whether Defendant was able to secure its systems during or after the breach.

9. Defendant's failure to timely report the Data Breach makes victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their private information.

10. Defendant knew or should have known that each victim of the Data Breach deserves prompt and efficient notice of the Data Breach and assistance in mitigating the effects of identity theft or misuse of their private information.

11. In failing to adequately protect consumers' private information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendant violated state law and harmed hundreds of thousands of its clients' customers.

12. Plaintiffs and the Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiffs and Members of the proposed Class trusted Defendant with their private information. But Defendant betrayed that trust when it failed to properly use up-to-date security practices to prevent the Data Breach.

13. Plaintiffs are current and former customers of Defendant's clients.

14. Plaintiffs provided Defendant or its clients with their personal identifying information ("PII") including their names, addresses, date of births, Social Security numbers, driver's license numbers, contact information (including phone number and email address), financial information (including credit card and account numbers), and insurance information. Upon information and belief, Plaintiffs' PII was managed through Motility's dealer management software, and Plaintiffs are victims of the Data Breach.

15. Motility provides dealer management software ("DMS")[5] to recreational vehicle, marine, bus, emergency vehicle, heavy truck and other dealerships.[6] Plaintiffs were customers of those dealerships. There was no legitimate reason to maintain Plaintiffs' PII once the vehicle or other transactions at issue were completed.

16. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before the Data Breach, the Plaintiffs' and the Class's private information and was exactly that—private. Not anymore. Now, their private information is permanently exposed and unsecure.

PARTIES

17. Plaintiff G. Scott Lockwood is a natural person and citizen of Montana, where he intends to remain.

18. Plaintiff Heather Reynicke is a natural person and citizen of New York, where she intends to remain.

19. Plaintiff Christopher Santora is a natural person and citizen of New York, where he intends to remain.

20. Plaintiff Donna Mathews is a natural person and citizen of Colorado, where she intends to remain.

21. Plaintiff John Langan is a natural person and citizen of Pennsylvania, where he intends to remain.

22. Plaintiff Nancy Langan is a natural person and citizen of Pennsylvania, where she intends to remain.

23. Plaintiff Stephen Duesler is a natural person and citizen of Georgia, where he

[5] *Motility Software Solutions: About us*, LinkedIn, https://www.linkedin.com/company/motilityss/about/ (last visited Nov. 4, 2025).

[6] *See Home Page*, Motility, https://www.motilitysoftware.com/ (last visited Nov. 4, 2025).

intends to remain.

24. Plaintiff Patrick Hubley is a natural person and citizen of North Carolina, where he intends to remain.

25. Plaintiff Peggy L. Koller is a natural person and citizen of Florida, where she intends to remain.

26. Defendant Motility Software Solutions, Inc., is a Delaware corporation with its headquarters and principal place of business located at 1 Reynolds Way, Kettering, Ohio 45420.

JURISDICTION AND VENUE

27. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Plaintiffs are citizens of different states than Defendant and there are over 100 members of the putative Class. After all, approximately 766,670 consumers were injured by the Data Breach.

28. This Court has personal jurisdiction over Defendant because it is headquartered in Kettering, Ohio, it regularly conducts business in Ohio and has sufficient minimum contacts in Ohio.

29. Venue is proper in this Court because Defendant's principal place of business is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

BACKGROUND

Defendant Collected and Stored the PII of Plaintiffs and the Class

30. Founded in 1984, Motility develops and markets software that provides, *inter alia*, a fully integrated document management system, customer relationship management tools,

accounting features, advanced reporting, as well as cloud hosting.[7] It flaunts itself as "providing best-in-class dealer management software ("DMS") to over 7,000 users and 800 rooftops" across the country.[8]

31. On information and belief, Motility accumulates highly private PII of its clients and their customers. Given its age, Motility has accrued over 40 years of data.

32. In collecting and maintaining its clients' customers' PII, Motility agreed it would safeguard the data in accordance with state law and federal law. After all, Plaintiffs and Class Members themselves took reasonable steps to secure their PII.

33. Motility understood the need to protect consumers' PII and prioritize its data security. In its Privacy Policy, Motility states:

> **Data Integrity**
>
> We will use Personal Information only in ways that align with the purposes for which it was originally collected, or if applicable, as [sic] ways it was later authorized by the individual. We will make reasonable efforts to ensure that personal data we hold is accurate, complete, and relevant for its intended purposes.
>
> **Data Security**
>
> We have safeguards in place to help prevent unauthorized access to and maintain security of information collected.
>
> **Notice if Personal Information is Compromised**
>
> We will notify you if we learn that your personal information is compromised.[9]

34. Additionally, Motility offers its clients a *FTC Safeguards Rule Amendments*

---

[7] *See Motility Software Solutions Overview,* PitchBook, https://pitchbook.com/profiles/company/226630-72#overview (last visited Nov. 4, 2025).

[8] *See* n.5.

[9] *Privacy Policy*, Motility (July 7, 2025), https://www.motilitysoftware.com/privacy-policy/ (last visited Nov. 4, 2025).

Playbook.[10] Motility informs its clients that, "In October 2021, the Federal Trade Commission (FTC) announced amendments to the Safeguards Rule. These amendments impact the security measures businesses that are considered non-banking financial institutions should implement for protecting consumer information. Effective June 9, 2023, these amendments impact the security measures that businesses, considered non-banking financial institutions, should implement to protect consumer information."[11] Motility offers to provide its clients with answers to frequently asked questions regarding the FTC's Safeguards Rule.[12]

35. Despite claiming to understand the FTC's rules and regulations regarding consumer data security and recognizing the need to protect its clients' data, on information and belief, Motility has not implemented reasonable cybersecurity safeguards or policies to protect the PII in its care or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Motility leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' PII.

Defendant Failed to Safeguard the PII of Plaintiffs and the Class

36. Plaintiffs are current and former customers of Defendant's clients and Data Breach victims.

37. As a condition of doing business with Defendant's clients, Plaintiffs provided Defendant with their PII, including but not limited to their names and Social Security numbers. Defendant used that PII to facilitate its business via its provision of DMS services to its clients.

38. On information and belief, Motility collects and maintains the PII of its clients

[10] *FTC Safeguards Rule Amendments Playbook*, Motility, https://www.motilitysoftware.com/resource-items/ftc-compliance-datasheet/ (last visited Nov. 4, 2025).

[11] *Id*.

[12] *Id*.

unencrypted in its computer systems.

39. In collecting and maintaining PII, Defendant implicitly and explicitly agreed that it would safeguard the data using reasonable means according to state and federal law.

40. According to Defendant's Breach Notice, on August 19, 2025, it "detected unusual activity within certain computer servers."[13] Defendant then launched an investigation, which determined that "an unauthorized actor deployed malware that encrypted a portion of our systems."[14] Defendant admits that "the actor may have *removed* limited files containing customers' personal data."[15]

41. In other words, Defendant's cyber and data security systems were completely inadequate in that it allowed cybercriminals to obtain and steal files containing a treasure trove of thousands of its clients' customers' highly sensitive PII.

42. Defendant states that the following types of PII were stolen in the Data Breach:

a. full names;

b. postal addresses;

c. email addresses;

d. telephone numbers;

e. dates of birth;

f. Social Security numbers; and

g. driver's license numbers.[16]

43. Through its inadequate security practices, Defendant exposed Plaintiffs' and the

[13] Ex. A at 1, 6.

[14] *Id.*

[15] *Id*

[16] *Id*.

Class's PII for theft and sale on the dark web.

44. Despite its duties to safeguard PII, Defendant did not in fact follow industry standard practices in securing its clients' customers' PII, as evidenced by the Data Breach.

45. On or around September 29, 2025—about six weeks after the Data Breach began—Defendant finally notified Class Members about the Data Breach.

46. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

47. And when Defendant did notify Plaintiffs and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, encouraging Plaintiffs and the Class to "remain vigilant and regularly review your credit card bills, bank statements, and credit reports for any unauthorized activity."[17]

48. Defendant failed in its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII stored in its systems. And thus, Defendant caused widespread injury and monetary damages.

49. Since the breach, Defendant states it "implemented additional security tools and measures to prevent recurrence" and that it "established dark net monitoring."[18]

50. But such simple declarations are insufficient to ensure that Plaintiffs' and Class Members' PII will be protected from additional exposure in a subsequent data breach.

51. Recognizing the risks of the Data Breach, Defendant has offered victims one year of identity monitoring.[19] However, even after implementing such credit monitoring services, the

[17] *Id.* at 2.

[18] *Id*. at 1, 6.

[19] *Id*. at 2.

risk of identity theft and unauthorized use of Plaintiffs' and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

52. Ultimately, Motility's failed efforts to adequately safeguard PII in its care subjects Plaintiffs and the Class to ongoing harm such as: opening new financial accounts in Class Members' names; committing financial theft; taking out loans in Class Members' names; using Class Members' information to obtain government benefits; and using the Class Members' PII to target them with phishing and other hacking intrusions.

53. As the Harvard Business Review notes, "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."

Cybercriminal Groups Claim Responsibility for the Data Breach

54. Two different cybercriminal groups have published Plaintiffs' and the Class's PII on the dark web.

55. First, the notorious cybercriminal group "PEAR" claimed credit for the Data Breach.[20]

56. The PEAR ransomware group, also known as Pure Extraction and Ransom, is a relatively new cyber extortion collective that emerged in June 2025. [21] Unlike many ransomware

[20] Paul Bischoff, *Auto dealership software company notifies 767,000 people of data breach claimed by ransomware gang*, Comparitech (Oct. 1, 2025), https://www.comparitech.com/news/auto-dealership-software-company-notifies-767000-people-of-data-breach-claimed-by-ransomware-gang/ (last visited Nov. 4, 2025).

[21] *Ransomware Strikes Accounting Firm: What Went Wrong and What Comes Next*, Cybernetic Global Intelligence (Aug. 20, 2025), https://www.cyberneticgi.com/ransomware-strikes-accounting-firm-what-went-wrong-next/ (last visited Nov. 4, 2025); *Threat Intelligence Report Aug. 5 – Aug. 11 2025: PEAR Ransomware,* Red Piranah, https://redpiranha.net/news/threat-intelligence-report-august-5-august-11-2025 (last visited Nov. 4, 2025).

operations that focus on encrypting data, PEAR's primary tactic is data theft and extortion.[22]

57. PEAR's main strategy is stealing sensitive data and threatening to leak it publicly rather than holding files for ransom. [23] This puts reputation and customer trust at risk, acting as the primary leverage for extortion.[24]

58. The group presents itself as a "responsible and disciplined" entity, claiming to punish organizations with poor cybersecurity hygiene. [25]

59. Thus, PEAR carefully selected Motility as its target to punish it for having particularly weak data security practices.

60. On or around September 13, 2025, PEAR announced that it had hacked Defendant via a post on its dark web portal.[26]

61. In its post, PEAR bragged that it had stolen 4.3TB (terabytes) of data from Defendant. [27]

[22] *Id*.

[23] *See Ransomware Strikes Accounting Firm*, Cybernetic Global Intelligence, *supra* n. 22.

[24] *Id*.

[25] DarkFeed (@ido_cohen2), *New Threat Actor Added: PEAR*, X (Aug. 7, 2025, at 04:23), https://x.com/ido_cohen2/status/1953371531121152379 (last visited Nov. 4, 2025).

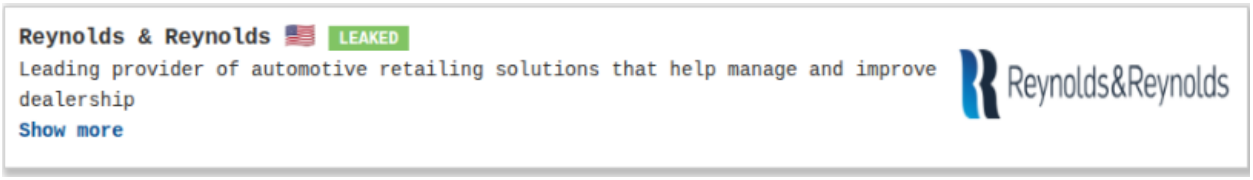
[26] FalconFeeds.io (@FalconFeeds.io), *Ransomware Alert: PEAR Ransomware has added 2 new victims to their dark web portal*, X (Sept. 13, 2025, at 09:00), https://x.com/FalconFeedsio/status/1966849464322453881 (last visited Nov. 4, 2025).

[27] *Id*., posted image.

62. PEAR's post further stated that the data stolen included "financials, HR, Business Operations, Partners and Vendors Data, Clients' and Customers private Data, Multiple Technical and Developments Data, Source Code, Mailboxes & Email Correspondence, and Databases."[28]

63. The above indicates that PEAR obtained more categories of PII than Defendant disclosed in its Breach Notice. 4.3 terabytes is a massive amount of data and can hold a huge variety of content. For context, 1 terabyte is equivalent to 1,000 gigabytes, and 1 gigabyte is equivalent to 1,000 megabytes. Thus, 4.3 terabytes is equivalent to 4,300,000 megabytes. The entire written works of Shakespeare could fit inside just 5 megabytes.[29]

64. In a subsequent post, PEAR labeled the PII stolen in the Data Breach as "leaked."[30]



65. Thus, on information and belief, PEAR has ***already published*** the PII stolen in the Data Breach on the dark web.

66. Furthermore, another ransomware group, "Brotherhood" also posted a link to Defendant's data on its "data leaks" site on the dark web.[31]

---

[28] *Id.*

[29] Paulette Kehely, *How Many documents In A Gigabyte?2024 statistics for litigators*, DWR eDiscovery (Apr. 2, 2020), https://www.digitalwarroom.com/blog/how-many-pages-in-a-gigabyte (last visited Nov. 4, 2025).

[30] Screen shot obtained from RansomLook at https://www.ransomlook.io/screenshots/pear/Reynolds%20%26%20Reynolds.png (last visited Nov. 4, 2025). RansomLook is an open-source project aimed at tracking ransomware-related posts and activities across various sites, forums, and Telegram channels. *See About*, RansomLook, https://www.ransomlook.io/about (last visited Nov. 4, 2025).

[31] Screen shot obtained from RansomLook, *supra*, n.31.

67. Brotherhood is a newly identified ransomware group.[32] It is unclear whether Brotherhood was involved in the Data Breach or whether the group obtained Plaintiffs' and the Class's data via PEAR's publication.

68. Defendant has made no public statements regarding PEAR, Brotherhood, or whether it made a ransom payment.

69. However, even if Defendant made a ransom payment, there is no guarantee that the PII stolen in the Data Breach will be deleted.[33] The stolen PII is valuable, and can easily be sold to another threat actor, so there is little incentive to delete it.[34]

70. Therefore, upon information and belief, Defendant's Breach Notice is intentionally

[32] ThreatMon (@MonThreat), *New Ransomware Group "Brotherhood" Targets Multiple Sectors*, X (Oct. 10, 2025, at 12:16), https://x.com/MonThreat/status/1976683352842191081 (last visited Nov. 4, 2025).

[33] Steve Adler, *Majority of Ransomware Victims That Pay a Ransom Suffer a Second Attack*, The HIPAA Journal (Feb. 23, 2024), https://www.hipaajournal.com/majority-of-ransomware-victims-that-pay-a-ransom-suffer-a-second-attack/ (last visited Nov. 4, 2025).

[34] *Id*.

misleading as it fails to inform Data Breach victims that their PII has been stolen by cybercriminals and posted on the dark web. Thus, Defendant's Breach Notice intentionally downplays the severity of the Data Breach and the threat it poses to hundreds of thousands of individuals.

Defendant Knew—or Should Have Known—of the Risk of a Data Breach

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

72. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

73. In 2024, 3,158 data breaches occurred, exposing approximately 1,350,835,988 sensitive records—a 211% increase year-over-year.[35]

74. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[36]

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

76. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Defendant failed to take

[35] *2024 Data Breach Report*, 6, Identity Theft Resource Center (Feb. 4, 2025), https://www.idtheftcenter.org/publication/2024-data-breach-report/ (last visited Nov. 4, 2025).

[36] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Nov. 4, 2025).

appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

77. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included extortion and threatening to release stolen data.

78. In light of the information readily available and accessible before the Data Breach, Defendant, knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack. Data breaches are so prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

Plaintiffs' Experiences and Injuries

Plaintiff G. Scott Lockwood

79. Plaintiff Lockwood a current customer of BRM, a client of Defendant, and a data breach victim.

80. As a condition of doing business with BRM, BRM required Plaintiff Lockwood to provide his PII, including at least his name, address, date of birth, driver's license number, Social Security number, contact information (including phone number and email address), financial information (including credit card and account numbers), and insurance information.

81. Plaintiff Lockwood provided his PII to Motility or its third party agent and trusted that the company would use reasonable measures to protect it according to state and federal law. Indeed, Motility represents that data entrusted to it will be secure.

82. Plaintiff Lockwood is very careful about sharing his sensitive PII. Plaintiff

Lockwood stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the Internet or any other unsecured source. Plaintiff Lockwood would not have entrusted his PII to Defendant or its third-party agent had he known of Motility's lax data security policies.

83. Plaintiff Lockwood does not recall ever learning that his PII was compromised in a data breach incident, other than the breach at issue in this case.

84. As a result of its inadequate cybersecurity measures and data destruction policies, Defendant exposed Plaintiff Lockwood's PII for theft by cybercriminals and sale on the dark web.

85. Plaintiff Lockwood's PII remains in Defendant's possession, and therefore Plaintiff Lockwood has an interest in ensuring that their PII is protected moving forward.

Plaintiff Heather Reynicke

86. Plaintiff Heather Reynicke is a former customer of Alpin Haus, a client of Defendant, and a data breach victim. On information and belief, Plaintiff Reynicke first provided her PII to Motility via in 2012.

87. As a condition of doing business with Alpin Haus, Alpin Haus required Plaintiff Reynicke to provide her PII, including at least her name, address, date of birth, driver's license number, Social Security number, contact information (including phone number and email address), financial information (including credit card and account numbers), and insurance information.

88. Plaintiff Reynicke provided her PII to Motility or its third party agent and trusted that the company would use reasonable measures to protect it according to state and federal law. Indeed, Motility represents that data entrusted to it will be secure.

89. Plaintiff Reynicke is very careful about sharing her sensitive PII. Plaintiff Reynicke stores any documents containing her PII in a safe and secure location. She has never knowingly

transmitted unencrypted sensitive PII over the Internet or any other unsecured source. Plaintiff Reynicke would not have entrusted her PII to Defendant or its third-party agent had she known of Motility's lax data security policies.

90. Plaintiff Reynicke does not recall ever learning that her PII was compromised in former a data breach incident, other than the breach at issue in this case.

91. As a result of its inadequate cybersecurity measures and data destruction policies, Defendant exposed Plaintiff Reynicke's PII for theft by cybercriminals and sale on the dark web.

92. Plaintiff Reynicke's PII remains in Defendant's possession, and therefore Plaintiff Reynicke has an interest in ensuring that their PII is protected moving forward.

Plaintiff Christopher Santora

93. Plaintiff Santora is a customer of Alpin Haus, a client of Defendant, and a data breach victim. On information and belief, Plaintiff Santora first provided his PII to Motility via Alpin Haus in 2019.

94. As a condition of doing business with Alpin Haus, Alpin Haus required Plaintiff Santora to provide his PII, including at least his name, date of birth, Social Security number, contact information (including phone number and email address), financial information (including credit card and account numbers), and insurance information.

95. Plaintiff Santora provided his PII to Motility or its third party agent and trusted that the company would use reasonable measures to protect it according to state and federal law. Indeed, Motility represents that data entrusted to it will be secure.

96. Plaintiff Santora is very careful about sharing his sensitive PII. Plaintiff Santora stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the Internet or any other unsecured source. Plaintiff

Santora would not have entrusted his PII to Defendant or its third-party agent had he known of Motility's lax data security policies.

97. As a result of its inadequate cybersecurity measures and data destruction policies, Defendant exposed Plaintiff Santora's PII for theft by cybercriminals and sale on the dark web.

98. Plaintiff Santora's PII remains in Defendant's possession, and therefore Plaintiff Santora has an interest in ensuring that their PII is protected moving forward.

Plaintiff Donna Mathews

99. Plaintiff Donna Mathews is a former customer of a client of Defendant. In March 2025, Plaintiff Mathews traded in a recreational vehicle at a dealership, and, on information and belief, transmitted her PII to Mobility via this transaction.

100. Plaintiff Mathews received Defendant's Breach Notice on or around early October 2025.

101. As a condition of doing business with Defendant's client, Defendant's client required Plaintiff Mathews to provide her PII, including at least her name, address, date of birth, driver's license number, Social Security number, contact information (including phone number and email address), financial information (including credit card and account numbers), and insurance information.

102. Plaintiff Mathews provided her PII to Motility or its third party agent and trusted that the company would use reasonable measures to protect it according to state and federal law. Indeed, Motility represents that data entrusted to it will be secure.

103. Plaintiff Mathews is very careful about sharing her sensitive PII. Plaintiff Mathews stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the Internet or any other unsecured source. Plaintiff

Mathews would not have entrusted her PII to Defendant or its third-party agent had she known of Motility's lax data security policies.

104. Plaintiff Mathews does not recall ever learning that her PII was compromised in former a data breach incident, other than the breach at issue in this case.

105. As a result of its inadequate cybersecurity measures and data destruction policies, Defendant exposed Plaintiff Mathews' PII for theft by cybercriminals and sale on the dark web.

106. Plaintiff Mathews' PII remains in Defendant's possession, and therefore Plaintiff Mathews has an interest in ensuring that their PII is protected moving forward.

Plaintiff John Langan

107. Plaintiff John Langan is and was customer of Defendant's client.

108. Plaintiff J. Langan received Defendant's Breach Notice dated October 1, 2025.

109. As a condition of doing business with Defendant's client, Defendant's client required Plaintiff J. Langan to provide his PII, including at least his name, address, date of birth, driver's license number, Social Security number, contact information (including phone number and email address), financial information (including credit card and account numbers), and insurance information.

110. Plaintiff J. Langan provided his PII to Motility or its third party agent and trusted that the company would use reasonable measures to protect it according to state and federal law. Indeed, Motility represents that data entrusted to it will be secure.

111. Plaintiff J. Langan is very careful about sharing his sensitive PII. Plaintiff J. Langan stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the Internet or any other unsecured source. Plaintiff J. Langan would not have entrusted his PII to Defendant or its third-party agent had he known of

Motility's lax data security policies.

112. Soon after the Data Breach, Plaintiff J. Langan began receiving an excessive number of spam calls on the same cell phone number provided to Defendant on his records. These calls are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, he believes that the calls are related to his PII stolen in the Data Breach.

113. As a result of its inadequate cybersecurity measures and data destruction policies, Defendant exposed Plaintiff J. Langan's PII for theft by cybercriminals and sale on the dark web.

114. Plaintiff J. Langan's PII remains in Defendant's possession, and therefore Plaintiff J. Langan has an interest in ensuring that their PII is protected moving forward.

Plaintiff Nancy Langan

115. Plaintiff Nancy Langan is and was customer of Defendant's client.

116. Plaintiff N. Langan received Defendant's Breach Notice dated October 1, 2025.

117. As a condition of doing business with Defendant's client, Defendant's client required Plaintiff N. Langan to provide her PII, including at least her name, address, date of birth, driver's license number, Social Security number, contact information (including phone number and email address), financial information (including credit card and account numbers), and insurance information.

118. Plaintiff N. Langan provided her PII to Motility or its third party agent and trusted that the company would use reasonable measures to protect it according to state and federal law. Indeed, Motility represents that data entrusted to it will be secure.

119. Plaintiff N. Langan is very careful about sharing her sensitive PII. Plaintiff N. Langan stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the Internet or any other unsecured source.

Plaintiff N. Langan would not have entrusted her PII to Defendant or its third-party agent had she known of Motility's lax data security policies.

120. Soon after the Data Breach, Plaintiff N. Langan began receiving an excessive number of spam calls on the same cell phone number provided to Defendant on her records. These calls are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, she believes that the calls are related to her PII stolen in the Data Breach.

121. As a result of its inadequate cybersecurity measures and data destruction policies, Defendant exposed Plaintiff N. Langan's PII for theft by cybercriminals and sale on the dark web.

122. Plaintiff N. Langan's PII remains in Defendant's possession, and therefore Plaintiff N. Langan has an interest in ensuring that their PII is protected moving forward.

Plaintiff Stephen Duesler

123. Plaintiff Stephen Duesler is and was customer of Defendant's client. On information and belief, Plaintiff Duesler first provided his PII to Motility in connection with the purchase of a recreational vehicle.

124. Plaintiff Duesler received Defendant's Breach Notice dated October 1, 2025.

125. As a condition of doing business with Defendant's client, Defendant's client required Plaintiff Duesler to provide his PII, including at least his name, address, date of birth, driver's license number, Social Security number, contact information (including phone number and email address), financial information (including credit card and account numbers), and insurance information.

126. Plaintiff Duesler provided his PII to Motility or its third party agent and trusted that the company would use reasonable measures to protect it according to state and federal law. Indeed, Motility represents that data entrusted to it will be secure.

127. Plaintiff Duesler is very careful about sharing his sensitive PII. Plaintiff Duesler stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the Internet or any other unsecured source. Plaintiff Duesler would not have entrusted his PII to Defendant or its third-party agent had he known of Motility's lax data security policies.

128. As a result of its inadequate cybersecurity measures and data destruction policies, Defendant exposed Plaintiff Duesler's PII for theft by cybercriminals and sale on the dark web.

129. Plaintiff Duesler's PII remains in Defendant's possession, and therefore Plaintiff Duesler has an interest in ensuring that their PII is protected moving forward.

Plaintiff Patrick Hubley

130. Plaintiff Patrick Hubley is and was a customer of Campers Inn RV, a client of Defendant, and a data breach victim. On information and belief, Plaintiff Hubley first provided his PII to Motility via Campers Inn RV in connection with that transaction in February 2019.

131. Plaintiff Hubley received Defendant's Breach Notice on or around early October 2025.

132. As a condition of doing business with Defendant's client, Defendant's client required Plaintiff Hubley to provide his PII, including at least his name, address, date of birth, driver's license number, Social Security number, contact information (including phone number and email address), financial information (including credit card and account numbers), and insurance information.

133. Plaintiff Hubley provided his PII to Motility or its third party agent and trusted that the company would use reasonable measures to protect it according to state and federal law. Indeed, Motility represents that data entrusted to it will be secure.

134. Plaintiff Hubley is very careful about sharing his sensitive PII. Plaintiff Hubley stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the Internet or any other unsecured source. Plaintiff Hubley would not have entrusted his PII to Defendant or its third-party agent had he known of Motility's lax data security policies.

135. Soon after the Data Breach, Plaintiff Hubley began receiving an excessive number of spam calls and emails on the same phone number and email provided to Defendant on his records. These calls and emails are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, he believes that the calls are related to his PII stolen in the Data Breach.

136. As a result of its inadequate cybersecurity measures and data destruction policies, Defendant exposed Plaintiff Hubley's PII for theft by cybercriminals and sale on the dark web.

137. Plaintiff Hubley's PII remains in Defendant's possession, and therefore Plaintiff Hubley has an interest in ensuring that their PII is protected moving forward.

Plaintiff Peggy L. Koller

138. Plaintiff Peggy L. Koller is and was a customer of a client of Defendant, and a data breach victim. On information and belief, Plaintiff Koller first provided her PII to Motility via an RV retailer in October 2021 and via a lightweight utility task vehicle retailer in December 2022.

139. Plaintiff Koller received Defendant's Breach Notice on or around early October 2025.

140. As a condition of doing business with Defendant's client, Defendant's client required Plaintiff Koller to provide her PII, including at least her name, address, date of birth, driver's license number, Social Security number, contact information (including phone number

and email address), and financial information (including credit card and account numbers).

141. Plaintiff Koller provided her PII to Motility or its third party agent and trusted that the company would use reasonable measures to protect it according to state and federal law. Indeed, Motility represents that data entrusted to it will be secure.

142. Plaintiff Koller is very careful about sharing her sensitive PII. Plaintiff Koller stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the Internet or any other unsecured source. Plaintiff Koller would not have entrusted her PII to Defendant or its third-party agent had she known of Motility's lax data security policies.

143. Soon after the Data Breach, Plaintiff Koller began receiving an excessive number of spam calls and emails on the same phone number and email provided to Defendant on her records. These calls and emails are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, he believes that the calls are related to her PII stolen in the Data Breach.

144. As a result of the Data Breach, Plaintiff Koller has had to spend over ten (10) hours dealing with the consequences of the Data Breach. This time and effort spent by Plaintiff Koller consists of: reviewing and protecting her accounts from fraud and identity theft and researching the potential consequences of the Data Breach. Plaintiff Koller is a forensic accountant and a Certified Fraud Examiner, and has applied her skills and expertise to addressing the consequences of this Data Breach and taking the steps necessary to mitigate its impact.

145. As a result of its inadequate cybersecurity measures and data destruction policies, Defendant exposed Plaintiff Koller's PII for theft by cybercriminals and sale on the dark web.

146. Plaintiff Koller's PII remains in Defendant's possession, and therefore Plaintiff

Hubley has an interest in ensuring that their PII is protected moving forward.

Allegations Common to All Plaintiffs

147. Given PEAR's and Brotherhood's dark web posts, Plaintiffs' PII has been published, or will be published for further theft, dissemination and/or sale on the dark web.

148. Defendant deprived Plaintiffs of the earliest opportunity to guard themselves against the Data Breach's effects by failing to promptly notify them about the Data Breach.

149. Plaintiffs suffered actual injury from the exposure of their PII —which violates their rights to privacy.

150. Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

151. Plaintiffs have spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing online account passwords, and monitoring credit information.

152. Plaintiffs will continue to spend valuable time they would have otherwise spent on other activities, including but not limited to, work and/or recreation. Plaintiffs' efforts were reasonable and necessary given that PEAR and Brotherhood have stolen their PII and published it on the dark web.

153. Plaintiffs fear for their personal financial security and uncertainty over what PII was exposed. Plaintiffs have and are experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach.

154. These emotional injuries were caused by Plaintiffs' loss of privacy and the exposure

to a heightened risk—of identity theft and fraud—which has been substantially elevated because PEAR advertised that it has stolen 4.3 terabytes of PII and leaked it on the dark web.

155. Plaintiffs are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties..

156. Plaintiffs have also experienced a substantial increase in scam and spam text messages, emails, and phone calls, all suggesting their PII is now in the hands of cybercriminals.

157. Once an individual's PII is for sale and access on the dark web, cybercriminals are able to use the stolen and compromised to gather and steal even more information.

158. Plaintiffs have a continuing interest in ensuring that their PII, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiffs and the Class Suffered Common Injuries and Damages Due to Defendant's Conduct

159. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

160. As a result of Defendant's failure to prevent the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, invasions of privacy, and emotional distress. Plaintiffs and the Class have suffered or are at an increased risk of suffering:

a. Identity theft and fraud;

b. The loss of the opportunity to control how their PII is used;

c. The diminution in value of their PII;

d. The compromise and continuing publication of their PII;

e. Out-of-pocket costs associated with the prevention, detection, recovery, and

remediation from identity theft or fraud;

f. Lost opportunity costs and lost wages associated with the time and effort expended 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 and fraud;

g. Delay in receipt of tax refund monies;

h. Unauthorized use of stolen PII; and

i. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

Plaintiffs Face a Significant Risk of Continued Identity Theft

161. Plaintiffs and Class Members are now at a heightened risk of identity theft for their lifetimes because of the Data Breach.

162. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201 (2013).

163. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id.*

164. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal individuals' personal data to monetize the information.

Criminals monetize the data by selling the stolen information on the Internet black market (aka the dark web) to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

165. The dark web is an unindexed layer of the Internet that requires special software or authentication to access.[37] Criminals in particular favour the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[38] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

166. The unencrypted PII of Plaintiffs and Class Members has or will end up for sale on the dark web because that is the modus operandi of hackers. In addition, unencrypted and detailed PII may fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the Plaintiffs' and Class Members' PII.

167. Theft of Social Security numbers also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of their SSN, and a new SSN will not be provided until after the victim has suffered the harm.

168. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other PII (e.g., name, address, date of birth) is akin to having

[37] Louis DeNicola, *What Is the Dark Web*, Experian (May 12, 2025), https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.

[38] *Id.*

a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[39]

169. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. An individual may not know that their Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

170. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[40]

171. It is within this context that Plaintiffs and all other Class Members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

172. Because a person's identity is akin to a puzzle with multiple data points, the more

[39] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, Time (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/ (last visited Nov. 4, 2025).

[40] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 12, 17 Journal of Systemics, Cybernetics and Informatics 5 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf (last visited Nov. 4, 2025).

accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

173. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

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

> Scammers use your Social Security number (SSN) to get other personal information about you. They can use your SSN and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your SSN until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought.[41]

175. Identity thieves can also use an individual's personal data and PII to file a fraudulent tax return or obtain a job in the victim's name.

176. One example of criminals piecing together bits and pieces of compromised PII to

[41] *Identity Theft and Your Social Security Number,* Social Security Administration, 1 (Oct. 2024), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Nov. 4, 2025).

create comprehensive dossiers on individuals is called "Fullz" packages.[42] These dossiers are both shockingly accurate and comprehensive. With "Fullz" packages, cybercriminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. For example, they can combine the stolen PII, and with unregulated data found elsewhere on the Internet (like phone numbers, emails, addresses, etc.).

177. The development of "Fullz" packages means that the PII exposed in the Data Breach can easily be linked to data of Plaintiffs and the Class that is available on the Internet. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and other Class Members' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

[42] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm,* Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm (last visited Nov. 4, 2025).

178. According to the FBI's Internet Crime Complaint Center (IC3) *2019 Internet Crime Report*, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[43]

179. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[44] Yet, Defendant failed to rapidly report to Plaintiffs and the Class that their PII was stolen. Defendant's failure to promptly and properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

180. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

181. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

182. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiffs and Class Members will need to remain vigilant for years or even decades to come.

---

[43] *2019 Internet Crime Report Released*, FBI, (Feb. 11, 2020) https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last visited Nov. 4, 2025).

[44] *Id.*

Loss of Time to Mitigate the Risk of Identify Theft and Fraud

183. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their PII was compromised, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the asset of time has been lost.

184. In the event that Plaintiffs and Class Members experience actual identity theft and fraud, the United States Government Accountability Office ("GAO") released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record.[45]

185. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must monitor their financial accounts for many years to mitigate that harm.

186. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover.

187. These efforts are consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud

[45] *Report to Congressional Requesters: Personal Information*, 2, GAO (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited Nov. 4, 2025).

alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[46]

188. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct that caused the Data Breach.

Diminished Value of PII

189. Personal data like PII is a valuable property right.[47]

190. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

191. An active and robust legitimate marketplace for personal information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[48]

192. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay on the dark web. Numerous sources cite such prices for stolen identity credentials.

193. For example, PII can be sold at a price ranging from $40 to $200, and bank details

---

[46] *See* FTC, *What To Do Right Away: What To Do Next*, IdentityTheft.gov, https://www.identitytheft.gov/Steps (last visited Sept. 25, 2025; currently unavailable due to federal appropriations lapse).

[47] *See, e.g.,* John T. Soma, *et al.*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[48] David Lazarus, *Shadowy data brokers make the most of their invisibility cloak*, L.A. Times (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Nov. 4, 2025).

have a price range of $50 to $200.[49] Experian reports that stolen credit card details can sell for $10 to $240 on the dark web.[50] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[51]

194. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[52] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $60 a year.[53]

195. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and black markets, has been damaged and diminished in its value by its unauthorized and likely release onto the dark web, where holds significant value for the threat actors.

196. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

---

[49] 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. 4, 2025).

[50] Ben Luthi, *Here's How What Your Data Sells for on the Dark Web*, Experian (June 30, 2025), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Nov. 4, 2025).

[51] *In the Dark*, VPNOverview, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Nov. 4, 2025).

[52] *The Personal Data Revolution,* Datacoup, Inc., https://datacoup.com/ (last visited Nov. 4, 2025).

[53] *Frequently Asked Questions: What rewards can I earn?*, Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Nov. 4, 2025).

Future Cost of Credit and Identify Theft Monitoring is Reasonable and Necessary

197. To date, Defendant has done little to provide Plaintiffs and Class Members with relief for the damages they have suffered due to the Data Breach.

198. Given the type of targeted attack in this case and sophisticated criminal activity, the type of information involved, and the modus operandi of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes—e.g., opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or insurance; or filing false unemployment claims.

199. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

200. The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

201. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

202. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

Lost Benefit of the Bargain

203. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain.

204. When agreeing to provide their PII, Plaintiffs and Class Members, as consumers and customers, understood and expected that they were, in part, paying for goods and data security to protect the PII they were required to provide.

205. Plaintiffs value data security. Indeed, consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[54]

206. In 2024, the technology and communications conglomerate Cisco published its annual *Consumer Privacy Survey*[55] and *Data Privacy Benchmark Study*.[56] Therein, Cisco reported the following:

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't

[54] *See* Janice Y. Tsai, *et al.*, *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, Abstract at 254, 22 Info. Sys. Res. 2, https://pubsonline.informs.org/doi/abs/10.1287/isre.1090.0260 (last visited Nov. 4, 2025).

[55] *Privacy Awareness: Consumers Taking Charge to Protect Personal: Cisco 2024 Consumer Privacy Survey*, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited Nov. 4, 2025).

[56] *Privacy as an Enabler of Customer Trust: Cisco 2024 Data Privacy Benchmark Study*, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2024.pdf (last visited Nov. 4, 2025).

trust with their data."[57]

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[58]

c. 89% of consumers stated that "I care about data privacy."[59]

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[60]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[61]

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[62]

Defendant Could Have Prevented the Data Breach

207. Data breaches are preventable.[63] 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."[64] She added that "[o]rganizations that collect, use, store, and share sensitive personal

[57] *Cisco 2024 Consumer Privacy Survey*, at 3, *supra*, n.59.

[58] *Cisco 2024 Data Privacy Benchmark Study*, at 3, *supra*, n.60.

[59] *Cisco 2024 Consumer Privacy Survey*, at 9, *supra*, n.59.

[60] *Id*.

[61] *Id*.

[62] *Id*. at 3, 11.

[63] Lucy L. Thompson, *Despite the Alarming Trends, Data Breaches Are Preventable*, in *Data Breach and Encryption Handbook* (Lucy Thompson, ed., 2012).

[64] *Id.* at 17.

data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[65]

208. "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." [66]

209. In a Data Breach like this one, many failures laid the groundwork for the Breach.

210. For example, the FTC has published guidelines that establish reasonable data security practices for businesses. The guidelines also emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

211. Additionally, several industry-standard best practices have been identified that—at a minimum—should be implemented by businesses like Defendant.

Defendant Failed to Adhere to FTC Guidelines

212. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

213. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

[65] *Id.* at 28.

[66] *Id.*

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

214. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

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

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

217. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

218. Defendant's failure is especially egregious here as Defendant expressly offers to assist its clients to understand the FTC's rules and regulations regarding consumer data security

by offering its clients its *FTC Safeguards Rule Amendments Playbook*.[67]

Defendant Failed to Follow Industry Standards

219. Experts studying cyber security routinely identify corporations as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

220. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant. These industry standards include: educating all employees regarding cybersecurity; strong passwords; multi-layer security, including firewalls, anti-virus, and anti- malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

221. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

222. Moreover, companies should retain personal data only as necessary, with legal justification. Personal data should not be stored beyond the time necessary to achieve its initial purpose of collection.

223. In line with industry standard practices, Defendant should have promptly deleted the data belonging to consumers after the vehicle or other transaction at issue transaction had ended.

224. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST

[67] *See* n.10, *supra*.

Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

225. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

226. Plaintiffs bring this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII was compromised in the Data Breach of Motility's network.

227. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including staff and immediate family.

228. Plaintiffs reserve the right to amend the class definition.

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

230. This action satisfies the numerosity, commonality, typicality, and adequacy requirements.

231. **Numerosity.** The Class Members are so numerous that joinder of all Class

Members is impracticable. According to Defendant, there are 766,670 affected persons.[68]

232. **Commonality and Predominance.** Plaintiffs' and the Class Members' claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class Members—for which a class wide proceeding can answer for all Class Members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's PII;

b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Defendant was negligent in maintaining, protecting, and securing PII;

d. if Defendant breached contract promises to safeguard Plaintiffs' and the Class's PII;

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiffs and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiffs and the Class are entitled to damages, treble damages, and or injunctive relief.

233. **Typicality.** Plaintiffs' claims are typical of Class Members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable

[68] *Data Breach Notifications*, Office of the Me. Att'y Gen, *supra*, n.2.

manner of notifying individuals about the Data Breach.

234. **Adequacy.** Plaintiffs will fairly and adequately protect the proposed Class's common interests. Their interests do not conflict with Class Members' interests. And Plaintiffs have retained counsel—including lead counsel—who are experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

235. **Appropriateness.** The likelihood that individual Class Members will prosecute separate actions is remote due to the time and expense necessary to prosecute an individual case. Plaintiffs are not aware of any litigation concerning this controversy already commenced by others who meet the criteria for class membership described above.

236. **Ascertainability.** All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some victims and sent them data breach notices.

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

237. Plaintiffs incorporate paragraphs 1 through 236 above as if fully set forth herein.

238. Defendant solicited, gathered, and stored the PII of Plaintiffs and the Class as part of the operation of its business and in order to gain revenues.

239. Upon accepting and storing the PII of Plaintiffs and Class Members, Defendant undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information and to use secure methods to do so.

240. Defendant had full knowledge of the sensitivity of the PII, the types of harm that Plaintiffs and Class Members could and would suffer if the PII was wrongfully disclosed, and the importance of adequate security.

241. Plaintiffs and Class Members were the foreseeable victims of any inadequate safety and security practices on the part of Defendant. Plaintiffs and the Class Members had no ability to protect their PII that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiffs and the Class.

242. Defendant was well aware of the fact that cyber criminals routinely target large corporations through cyberattacks in an attempt to steal sensitive personal information.

243. Defendant owed Plaintiffs and the Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data and providing notification to Plaintiffs and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

244. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures also have recognized the existence of a specific duty to reasonably safeguard personal information.

245. Defendant had duties to protect and safeguard the PII of Plaintiffs and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive PII. Additional duties that Defendant owed Plaintiffs and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, email accounts, protocols, policies, procedures and practices to ensure that Plaintiffs' and

Class Members' PII was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiffs' and Class Members' PII in its possession by using reasonable and adequate security procedures and systems;

c. To implement processes to quickly detect a data breach, security incident, or intrusion involving its business email system, networks and servers; and

d. To promptly notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

246. Defendant's common law duties to Plaintiffs and the Class are independent from and untethered by any contract.

247. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the PII that Plaintiffs and the Class had entrusted to it.

248. Defendant breached its duty of care by failing to adequately protect Plaintiffs' and Class Members' PII. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the PII in its possession;

b. Failing to protect the PII in its possession by using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees to avoid phishing emails;

d. Failing to use adequate email security systems, including industry standard SPAM filters, DMARC enforcement, and/or Sender Policy Framework enforcement to protect against phishing emails;

e. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII;

f. Failing to adequately train its employees to not store PII longer than absolutely necessary for the specific purpose that it was sent or received;

g. Failing to consistently enforce security policies aimed at protecting Plaintiffs' and the Class's PII;

h. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

i. Failing to promptly notify Plaintiffs and Class Members of the Data Breach that affected their PII.

249. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

250. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

251. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the PII of Plaintiffs and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiffs and Class Members while it was within Defendant's possession and control.

252. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class Members, Defendant prevented Plaintiffs and Class Members from taking meaningful, proactive steps toward securing their PII and mitigating damages.

253. As a result of the Data Breach, Plaintiffs and Class Members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to fraudulent activity, closely monitoring bank account activity, and examining credit reports and statements sent from providers and their insurance companies.

254. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

255. The damages Plaintiffs and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

256. In addition to its duties under common law, Defendant had additional duties imposed by statute and regulations, including the duties under the FTC Act. The harms which occurred as a result of Defendant's failure to observe these duties, including the loss of privacy, lost time and expense, and significant risk of identity theft are the types of harm that these statutes and regulations intended to prevent.

257. Defendant violated these statutes when it engaged in the actions and omissions alleged herein, and Plaintiffs' and Class Members' injuries were a direct and proximate result of Defendant's violations of these statutes. Plaintiffs therefore are entitled to the evidentiary presumptions for negligence per se.

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

259. The FTC Act prohibits "unfair practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described

above also formed part of the basis of Defendant's duty in this regard.

260. Defendant gathered and stored the PII of Plaintiffs and the Class as part of its business, which affect commerce.

261. Defendant violated the FTC Act by failing to use reasonable measures to protect the PII of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

262. Defendant breached its duties to Plaintiffs and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiffs' and Class Members' PII, and by failing to provide prompt and specific notice without reasonable delay.

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

264. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against.

265. Defendant breached its duties to Plaintiffs and the Class under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and the Class's PII.

266. Defendant breached its duties to Plaintiffs and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiffs and the Class.

267. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

268. The injury and harm that Plaintiffs and Class Members suffered (as alleged above)

was the direct and proximate result of Defendant's negligence.

269. Plaintiffs and the Class have suffered injury and are entitled to actual and punitive damages in amounts to be proven at trial.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

270. Plaintiffs incorporate paragraphs 1 through 236 above as if fully set forth herein.

271. Plaintiffs bring this claim in the alternative to claims arising in tort or equity.

272. Through their course of conduct, Defendant, Plaintiffs and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' PII.

273. Defendant required Plaintiffs and Class Members to provide, or authorize the transfer of, their PII in order for Defendant's clients to provide services. In exchange, Defendant entered into implied contracts with Plaintiffs and Class Members in which Defendant agreed to implement adequate data security measures to protect Plaintiffs' and Class Members' PII and to timely notify them in the event of a data breach.

274. Defendant solicited and invited Plaintiffs and Class Members to provide their PII as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their PII to Defendant.

275. As a condition of being customers of Defendant's clients, Plaintiffs and Class Members provided and entrusted their PII to Defendant. In so doing, they entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen.

276. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their PII to Defendant, in exchange for, amongst other things, the protection of their PII.

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

278. Implicit in the agreement between Plaintiffs and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

279. Defendant's implied promises are evidenced by its public-facing privacy policy.

280. Plaintiffs and the members of the Class would not have entrusted their PII to Defendant or its third-party agents and partners in the absence of such an agreement with Defendant.

281. Defendant accepted possession of Plaintiffs' and Class Members' PII.

282. Had Defendant or its third-party agents and partners disclosed to Plaintiffs and Class Members that Defendant did not have adequate computer systems and security practices to secure consumers' PII, Plaintiffs and Class Members would not have provided their PII to Defendant or its third-party agents and partners.

283. Defendant recognized that consumers' PII is highly sensitive and must be protected, and that this was of material importance as part of the bargain to Plaintiffs and Class Members.

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

285. Defendant materially breached the contracts it had entered with Plaintiffs and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusions into its computer systems that compromised such information. Defendant also breached the implied contracts with Plaintiffs and members of the Class by:

a. Failing to properly safeguard and protect Plaintiffs' and Class Members' PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

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

(h) the continued and substantial risk to Plaintiffs' and Class Members' PII, which remains in the Defendant's possession with inadequate measures to protect Plaintiffs' and Class Members' PII.

287. Additionally, the covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

288. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

289. In these and other ways, Defendant violated its duty of good faith and fair dealing.

290. Plaintiffs and Members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

291. Plaintiffs, on behalf of themselves and the Class, seek compensatory damages for breach of implied contract, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

292. Plaintiffs incorporate paragraphs 1 through 236 above as if fully set forth herein.

293. Plaintiffs bring this claim in the alternative to claims arising in contract or tort.

294. Upon information and belief, Defendant funds its data security measures from its general revenue, including payments made by or on behalf of Plaintiffs and the Class Members.

295. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

296. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased services from Defendant and/or its agents and in so doing provided Defendant or its agents with their PII. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

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

298. Plaintiffs and Class Members conferred a monetary benefit on Defendant, by paying Defendant or its third-party agents and partners as part of Defendant and/or its agents rendering services, a portion of which was to have been used for data security measures to secure Plaintiffs' and Class Members' PII, and by providing Defendant with their valuable PII.

299. Defendant was enriched by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to avoid the data security obligations at the expense of Plaintiffs and the Class by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

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

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

302. If Plaintiffs and Class Members had known that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant either directly or through its third-party agents and partners.

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

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

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

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

FOURTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

307. Plaintiffs incorporate paragraphs 1 through 236 above as if fully set forth herein.

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

309. Defendant owed a duty to Plaintiffs and Class Member to keep their PII confidential.

310. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiffs' and Class Members' PII is highly offensive to a reasonable person. It constitutes an invasion of privacy both by disclosure of nonpublic facts, and intrusion upon seclusion.

311. The decision to store PII in a way that is vulnerable to foreseeable threats is highly offensive to a reasonable person. The subsequent publication of the stolen PII on the Dark Web is also highly offensive to a reasonable person.

312. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class Members disclosed their sensitive and confidential information to Defendant or its third-party agents and partners privately, with the intention that their information

would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

313. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

314. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

315. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs' and the Class Members in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

316. Defendant had notice and knew or should have known that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class Members.

317. Because Defendant failed to properly safeguard Plaintiffs' and Class Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

318. As a proximate result of Defendant's acts and omissions, the PII of Plaintiffs and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

319. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII is still maintained by Defendant with their inadequate cybersecurity system and policies.

320. Plaintiffs and Class Members have no adequate remedy at law for the injuries

relating to Defendant's continued possession of their PII. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiffs and the Class.

321. Plaintiffs and Class Members seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' PII.

322. Plaintiffs and Class Members seek nominal and/or compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

FIFTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiffs and the Class)

323. Plaintiffs incorporate by reference paragraphs 1 through 236 above as if fully set forth herein.

324. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

325. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiffs allege that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiffs and Class Members continue to suffer injury from the ongoing threat of fraud and identity theft.

326. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed—and continues to owe—a legal duty to use reasonable

data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it;

d. Defendant's breaches of its duties caused—and continues to cause—injuries to Plaintiffs and Class Members; and

e. Defendant must provide Plaintiffs and Class Members with lifelong credit monitoring services.

327. The Court should issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

328. The Court should also issue injunctive relief requiring Defendant to provide Plaintiffs and Class Members with lifelong credit monitoring services.

329. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences another data breach.

330. And if another breach occurs, Plaintiffs and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiffs' and Class Members' injuries.

331. If an injunction is not issued, the resulting hardship to Plaintiffs and Class Members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

332. An injunction would benefit the public by preventing another data breach—thus

preventing further injuries to Plaintiffs, Class Members, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of all others similarly situated, prays for relief as follows:

a. For an order certifying the Class, and naming Plaintiffs as representatives of the Class, and Plaintiffs' attorneys as Class Counsel;

b. For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiffs reasonable attorneys' fees, costs, and expenses as otherwise allowed by law;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, individually and on behalf of the putative Class, demand a trial by jury of all claims so triable.

Dated: November 9, 2025

Respectfully submitted,

/s/ *Terence R. Coates*
Terence R. Coates (0085579)
Dylan J. Gould (0097954)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, Ohio 45202
Telephone: (513) 651-3700
Facsimile: (513) 665-0219

tcoates@msdlegal.com
dgould@msdlegal.com

Raina Borrelli (*pro hac vice*)
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
raina@straussborrelli.com

Gary M. Klinger (*pro hac vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN LLC
227 W. Monroe Street, Suite 2100
Chicago, IL 6060
Phone: (866) 252-0878
gklinger@milberg.com

Interim Class Counsel

Jeff Ostrow (*pro hac vice*)
KOPELOWITZ OSTROW P.A.
1 W. Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 525-4100
ostrow@kolawyers.com

Marc H. Edelson*
Liberato P. Verderame*
EDELSON LECHTZIN LLP
411 S. State Street, Suite N300
Newtown, PA 18940
T: (215) 867-2399
medelson@edelson-law.com
lverderame@edelson-law.com

Robert R. Sparks (0073573)
rrsparks@strausstroy.com
STRAUSS TROY CO., LPA
150 E. Fourth St, 4th Floor
Cincinnati, OH 45202-4018
Phone: 513-621-2120
Fax: 513-241-8259

JOHN A. YANCHUNIS*
jyanchunis@forthepeople.com
RONALD PODOLNY*
ronald.podolny@forthepeople.com
MORGAN & MORGAN COMPLEX
LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Phone: (813) 275-5272
Fax: (813) 222-4736

Additional Counsel for
Plaintiffs and the Proposed Class

* Motion for admission *pro hac vice* forthcoming

CERTIFICATE OF SERVICE

I hereby certify that on November 9, 2025, I served the foregoing upon counsel of record for all parties by filing it with the court's electronic-filing system in accordance with Fed. R. Civ. P. 5(b)(2)(E).

/s/ Terence R. Coates
Terence R. Coates (0085579)