

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO**

JED RUDD, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

UNION HOME MORTGAGE CORP.,

Defendant.

Case No. 1:25-cv-01874

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Jed Rudd (“Plaintiff”), on behalf of all others similarly situated, by and through his undersigned counsel, brings this Class Action Complaint against Union Home Mortgage Corp. (“Defendant”). Plaintiff alleges the following upon information and belief based on and the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiff and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted Defendant with sensitive Personally Identifiable Information (“PII”¹ or “Private Information”) and that was impacted in a cyber incident (the “Data Breach” or the “Breach”).

2. Plaintiff’s claims arise from Defendant’s failure to properly secure and safeguard Private Information that was entrusted to it, and its accompanying responsibility to store and transfer that information.

¹ Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

3. Defendant is a privately held American mortgage lending company founded in 1970, based in Strongsville, Ohio.

4. On June 25, 2025, Defendant learned that an unauthorized third-party accessed its IT Network.² In response, Defendant launched an investigation to determine the nature and scope of the Data Breach.³

5. On August, 19, 2025, Defendant learned that Private Information contained in its IT Network was accessed by the unauthorized third-party.⁴

6. Upon information and belief, the following types of Private Information were exposed as a result of the Data Breach: name, Social Security number, home address, date of birth, driver's license/state ID, and/or passport.⁵

7. On August 29, 2025 – two months after Defendant was made aware of the Data Breach - Defendant issued a public disclosure about the Data Breach and began sending notice letters (“Notice”) to impacted individuals.

8. Defendant failed to take precautions designed to keep individuals’ Private Information secure.

9. Defendant owed Plaintiff and Class Members a duty to take all reasonable and necessary measures to keep the Private Information collected safe and secure from unauthorized access. Defendant solicited, collected, used, and derived a benefit from the Private Information, yet breached its duty by failing to implement or maintain adequate security practices.

10. Defendant admits that information in its system was accessed by unauthorized

² Exhibit A, Plaintiff Rudd’s Notice Letter.

³ *Id.*

⁴ *Id.*

⁵ *Id.*

individuals, though it provided little information regarding how the Data Breach occurred.

11. The sensitive nature of the data exposed through the Data Breach signifies that Plaintiff and Class Members have suffered irreparable harm. Plaintiff and Class Members have lost the ability to control their private information and are subject to an increased risk of identity theft.

12. Defendant, despite having the financial wherewithal and personnel necessary to prevent the Data Breach, nevertheless failed to use reasonable security procedures and practice appropriate to the nature of the sensitive, unencrypted information it maintained for Plaintiff and Class Members, causing the exposure of Plaintiff's and Class Members' Private Information.

13. As a result of Defendant's inadequate digital security and notice process, Plaintiff's and Class Members' Private Information was exposed to criminals. Plaintiff and the Class Members have suffered and will continue to suffer injuries including: financial losses caused by misuse of their Private Information; the loss or diminished value of their Private Information as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal and financial information.

14. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; (iii) effectively secure hardware containing protected Private Information using reasonable and adequate security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiff and Class Members of the Data Breach. Defendant's conduct amounts to at least negligence and violates federal and state statutes.

15. Plaintiff brings this action individually and on behalf of a Nationwide Class of

similarly situated individuals against Defendant for: negligence; negligence *per se*; unjust enrichment, and breach of implied contract.

16. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of himself, and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

Plaintiff

17. Plaintiff is a citizen and resident of Aledo, Texas.

Defendant

18. Defendant is an Ohio corporation, having its principal place of business at 8241 Dow Circle West, Strongsville, Ohio 44136.

JURISDICTION AND VENUE

19. 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. At least one Class Member is diverse from Defendant, including Plaintiff, and there are over 100 putative Class Members.

20. This Court has personal jurisdiction over Defendant because Defendant is headquartered in this District, regularly conduct business in this District, and thus, has sufficient minimum contacts in this District.

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

FACTUAL ALLEGATIONS

A. Background on Defendant

22. Defendant is a privately held American mortgage lending company founded in 1970, based in Strongsville, Ohio.

23. Upon information and belief, Defendant made promises and representations to individuals', including Plaintiff and Class Members, that the Private Information collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.

24. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

25. As a result of collecting and storing the Private Information of Plaintiff and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiff's and the Class Members' Private Information from disclosure to third parties.

B. The Data Breach

26. On June 25, 2025, Defendant learned that an unauthorized third-party accessed its IT Network.⁶ In response, Defendant launched an investigation to determine the nature and scope of the Data Breach.⁷

27. On August, 19, 2025, Defendant learned that Private Information contained in its

⁶ Exhibit A, Plaintiff Rudd's Notice Letter.

⁷ *Id.*

IT Network was accessed by the unauthorized third-party.⁸

28. Upon information and belief, the following types of Private Information were exposed as a result of the Data Breach: name, Social Security number, home address, date of birth, driver's license/state ID, and/or passport.⁹

29. On August 29, 2025 – two months after Defendant was made aware of the Data Breach - Defendant issued a public disclosure about the Data Breach and began sending Notice to impacted individuals.

30. Defendant failed to take precautions designed to keep individuals' Private Information secure.

31. While Defendant sought to minimize the damage caused by the Data Breach, it cannot and has not denied that there was unauthorized access to the sensitive Private Information of Plaintiff and Class Members.

32. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

C. Defendant's Failure to Prevent, Identify, and Timely Report the Data Breach

33. Defendant admits that an unauthorized third party accessed IT Network. Defendant failed to take adequate measures to protect its computer systems against unauthorized access.

34. The Private Information that Defendant allowed to be exposed in the Data Breach is the type of private information that Defendant knew or should have known would be the target of cyberattacks.

35. Despite its own knowledge of the inherent risks of cyberattacks, and

⁸ *Id.*

⁹ *Id.*

notwithstanding the FTC's data security principles and practices,¹⁰ Defendant failed to disclose that its systems and security practices were inadequate to reasonably safeguard Plaintiff and Class Members Private Information.

36. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.¹¹ Immediate notification of a Data Breach is critical so that those impacted can take measures to protect themselves.

37. Here, Defendant waited two months after being made aware of the Data Breach to notify impacted individuals.

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

38. It is well known that Private Information is an invaluable commodity and a frequent target of hackers.

39. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years. In light of past high profile data breaches at industry-leading companies, including, for example, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or, if acting as a reasonable business, should have known that the Private Information it collected and maintained would be vulnerable to and targeted by cybercriminals.

40. In 2024, a 3,158 data breaches occurred, exposing approximately 1,350,835,988

¹⁰ FTC, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Sept. 8, 2025).

¹¹ *Id.*

sensitive records—a 211% increase year-over-year.¹²

41. 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.¹³

42. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and Defendant.

43. 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 Private Information private and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

44. 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.

45. 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 Plaintiff's and Class Members' Private Information 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

¹² Identity Theft Resource Center, *ITRC 2024 Data Breach Annual Report* (Feb. 4, 2025), <https://www.idtheftcenter.org/publication/2024-data-breach-report/> (last visited Sept. 8, 2025).

¹³ 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 Sept. 8, 2025).

experiencing a data breach entirely foreseeable to Defendant.

E. Plaintiff's Experience and Injuries

46. Plaintiff is an employee of Defendant and a data breach victim.

47. As a condition of receiving employment services, Plaintiff was required to provide his Private Information to Defendant.

48. Plaintiff provided his Private Information to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

49. On August 29, 2025, Defendant sent Plaintiff a Notice informing him that his Private Information was compromised in the Data Breach.

50. As a result of its inadequate cybersecurity measures and data destruction policies, Defendant exposed Plaintiff's Private Information for theft by cybercriminals and given the purpose of the hack, for sale on the Dark Web.

51. Defendant deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to promptly notify her about the Data Breach.

52. Plaintiff suffered actual injury from the exposure of his Private Information — which violates his rights to privacy.

53. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

54. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts to mitigate its impact, including but not limited to researching the Data Breach, reviewing credit card and financial account statements and monitoring his credit information.

55. Plaintiff will continue to spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff fears for his personal financial security

and uncertainty over what Private Information was exposed. Plaintiff has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

56. And in the aftermath of the Data Breach, Plaintiff has suffered from a spike in spam and scam emails, text messages, and emails, and has received alerts that his Private Information has appeared on the Dark Web.

57. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties. This injury is worsened by Defendant's failure to promptly inform Plaintiff about the Data Breach.

58. Once an individual's Private Information 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.¹⁴ Plaintiff's Private Information was compromised as a result of the Data Breach.

59. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

60. Plaintiff also has a continuing interest in lifetime credit monitoring and identity theft monitoring on account of the Data Breach.

F. Plaintiff and the Class Suffered Common Injuries and Damages Due to Defendant's Conduct

61. Defendant's failure to implement or maintain adequate data security measures for

¹⁴ Ryan Toohill, *What do Hackers do with Stolen Information*, Aura (Sept. 5, 2023), <https://www.aura.com/learn/what-do-hackers-do-with-stolen-information> (last visited Sept. 8, 2025).

Plaintiff's and Class Members' Private Information directly and proximately injured Plaintiff and Class Members by the resulting disclosure of their Private Information in the Data Breach.

62. Because of Defendant's failure to prevent the Data Breach, Plaintiff and Class members suffered—and will continue to suffer—damages. These damages include, inter alia, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

- a. identity theft and fraud;
- b. loss of time to mitigate the risk of identity theft and fraud
- c. diminution in value of their Private Information;
- d. out-of-pocket costs from trying to prevent, detect, and recover from identity theft and fraud;
- e. lost benefit of the bargain and opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, inter alia, preventing, detecting, contesting, and recovering from identify theft and fraud;
- f. delay in receipt of tax refund monies;
- g. loss of the opportunity to control how their Private Information is used;
- h. compromise and continuing publication of their Private Information;
- i. unauthorized use of their stolen Private Information;
- j. invasion of privacy; and
- k. continued risk to their Private Information—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the Private Information.

G. Significant Risk of Continued Identity Theft

63. Plaintiff and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

64. 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).

65. 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.*

66. 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.

67. The dark web is an unindexed layer of the internet that requires special software or authentication to access.¹⁵ 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

¹⁵ Louis DeNicola, *What Is the Dark Web?*, Experian (May 12, 2021), <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/> (last visited Sept. 8, 2025).

ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.¹⁶ This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

68. The unencrypted Private Information of Plaintiff 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 Private Information may fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Plaintiff's and Class Members' Private Information.

69. The value of Plaintiff's and Class's Private Information on the black market is considerable. Stolen Private Information trades on the black market for years and is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen Private Information can be worth up to \$1,000.00 depending on the type of information obtained. criminals frequently post and sell stolen information openly and directly on the "dark web"—further exposing the information.

70. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the Private Information far and wide.

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

72. 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

¹⁶ *Id.*

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.

73. Identity thieves can also use an individual's personal data and Private Information to obtain a driver's license or official identification card in the victim's name but with the thief's picture; rent a house or receive medical services in the victim's name; use the victim's Private Information to obtain government benefits; and may even give the victim's personal information to police during an arrest resulting in criminal proceedings commenced under the victim's name. In addition, identity thieves may obtain a job using the victim's information, and file a fraudulent tax return using the victim's information.¹⁷

74. One example of criminals piecing together bits and pieces of compromised Private Information to create comprehensive dossiers on individuals is called "Fullz" packages.¹⁸ These dossiers are both shockingly accurate and comprehensive. With "Fullz" packages, cybercriminals can cross-reference two sources of Private Information 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 Private

¹⁷ Social Security Administration, *Identity Theft and Your Social Security Number*, 4 (Oct. 2024), <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Sept. 8, 2025).

¹⁸ "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 Sept. 8, 2025).

Information, and with unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

75. The development of “Fullz” packages means that the Private Information exposed in the Data Breach can easily be linked to data of Plaintiff 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 Private Information 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 Plaintiff and Class members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class members’ stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

76. 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.¹⁹

77. Further, according to the same report, “rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good.”²⁰ Yet, Defendant failed to rapidly report to Plaintiff and the Class that their Private Information was stolen. Defendant’s failure to promptly and properly notify Plaintiff and Class members of the Data Breach exacerbated Plaintiff and Class members’ injury by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take necessary steps to mitigate the harm caused by the Data Breach.

¹⁹ FBI, *2019 Internet Crime Report*, FBI.gov (Feb. 11, 2020), <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120> (last visited Sept. 8, 2025).

²⁰ *Id.*

78. 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.

79. 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 Private Information. 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.

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

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

81. 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 Private Information was compromised, as in this Data Breach, 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 or 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.

82. In the event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office 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.

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

84. Plaintiff 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.

85. 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 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.²¹

86. Once Private Information 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, Plaintiff 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.

I. Diminished Value of Private Information

87. Personal data like Private Information is a valuable property right.²²

88. Its value is axiomatic, considering the value of Big Data in corporate America and

²¹ See FTC, *What To Do Right Away: What To Do Next*, IdentityTheft.gov, <https://www.identitytheft.gov/Steps> (last visited Sept. 8, 2025).

²² See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII/PHI”) Equals the “Value” of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (“PII/PHI, 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).

the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

89. An active and robust legitimate marketplace for personal information also exists. In 2019, the data brokering industry was worth roughly \$200 billion.²³

90. 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.²⁴ Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$60 a year.²⁵

91. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, 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.

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

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

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

²³ David Lazarus, *Shadowy data brokers make the most of their invisibility cloak*, Los Angeles Times (Nov. 5, 2019), <https://www.latimes.com/business/story/2019-11-05/column-data-brokers> (last visited Sept. 8, 2025).

²⁴ Datacoup, Inc., *The personal data revolution*, <https://datacoup.com> (last visited Sept. 8, 2025).

²⁵ Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, <https://computermobilepanel.nielsen.com/ui/US/en/faqs.html> (last visited Sept. 8, 2025).

94. 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 Private Information 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.

95. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that her 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.

96. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel their cards and request a replacement.²⁶

97. The information disclosed in this Data Breach is impossible to “close” and difficult, if not impossible, to change.

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

99. 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

²⁶ Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web, New Report Finds*, Forbes (Mar 25, 2020), <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1> (last visited Sept. 8, 2025).

minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

K. Lost Benefit of the Bargain

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

101. When agreeing to provide their Private Information, which was a condition precedent to obtain services from Defendant, Plaintiff and Class Members, understood and expected that they were, in part, paying for services or receiving lesser wages, in exchange for data security to protect the Private Information they were required to provide.

102. Plaintiff values data security. Indeed, data security is an important consideration of seeking financial services.

103. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."²⁷ Therein, Cisco reported the following:

"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 trust with their data."²⁸

104. "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."²⁹ 89% of consumers stated that "I care about data privacy."³⁰ 83% of consumers

²⁷ Cisco, *Privacy Awareness: Consumers Taking Charge to Protect Personal*, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited Sept. 8, 2025).

²⁸ *Id.* at 3.

²⁹ *Id.*

³⁰ *Id.* at 9.

declared that “I am willing to spend time and money to protect data” and that “I expect to pay more” for privacy.³¹

105. Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services of a lesser value than what they reasonably expected to receive under the bargains struck with Defendant.

L. Defendant Could Have Prevented the Data Breach

106. Data breaches are preventable.³² 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.”³³ She added that “[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised”³⁴

107. “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.”³⁵

108. In a Data Breach like the one here, many failures laid the groundwork for the Breach. 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 risks.

³¹ *Id.*

³² Lucy L. Thomson, *Despite the Alarming Trends, Cybersecurity Incidents Are Preventable*, in *Cybersecurity Incident and Encryption Handbook* (Lucy Thompson, ed., 2012).

³³ *Id.* at 17.

³⁴ *Id.* at 28.

³⁵ *Id.*

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

M. Defendant Failed to Adhere to FTC Guidelines

110. 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 Private Information.

111. 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: (i) protect the personal information that they keep; (ii) properly dispose of personal information that is no longer needed; (iii) encrypt information stored on computer networks; (iv) understand their network’s vulnerabilities; and (v) implement policies to correct security problems.

112. 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.

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

114. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect individuals 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.

115. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff and Class Members Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

N. Defendant Failed to Follow Industry Standards

128. Experts studying cybersecurity routinely identify financial corporations as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

129. 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.

130. 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.

131. 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. In line with industry standard practices, Defendant should have promptly deleted any data it no longer needed to provide services to Plaintiff and the Class.

132. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

133. 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.

O. The Harm Caused by the Data Breach Now and Going Forward

116. Victims of data breaches are susceptible to becoming victims of identity theft. 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(9). When “identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance.”³⁶

117. The type of data that may have been accessed and compromised here can be used to perpetrate fraud and identity theft.

118. Plaintiff and Class Members face a substantial risk of identity theft given that their

³⁶ New York State Police, *Prevention and Preparedness: Identity Theft*, <https://troopers.ny.gov/prevention-and-preparedness> (last visited Sept. 8, 2025).

Private Information was compromised in the Data Breach.

119. Stolen Private Information is often trafficked on the “dark web,” a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the “dark web” due to this encryption, which allows users and criminals to conceal their identities and online activity.

120. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, the stolen information often ends up on the dark web where malicious actors buy and sell that information for profit.³⁷

121. For example, when the U.S. Department of Justice announced their seizure of AlphaBay—the largest online “dark market”—in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person’s identity.”³⁸ Marketplaces similar to the now-defunct AlphaBay continue to be “awash with [PII] belonging to victims from countries all over the world.”³⁹

122. PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.⁴⁰ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.⁴¹

³⁷ IdentityForce, *Shining a Light on the Dark Web with Identity Monitoring* (Feb. 1, 2020), <https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring> (last visited Sept. 8, 2025).

³⁸ Armor Team, *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor (Apr. 3, 2018), <https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/> (last visited Sept. 8, 2025).

³⁹ *Id.*

⁴⁰ *Id.*

⁴¹ Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited Sept. 8, 2025).

123. As a result of the Data Breach, the Private Information of Plaintiff and Class Members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class Members, or likely to be suffered as a direct result of Defendant's Data Breach, include: (a) theft of their Private Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard their Private Information against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further injurious breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

124. In addition to a remedy for economic harm, Plaintiff and Class Members maintain an interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

125. Defendant disregarded the rights of Plaintiff and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to

safeguard Plaintiff's and Class Members' Private Information; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

126. The actual and adverse effects to Plaintiff and Class Members, including the imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly or proximately caused by Defendant's wrongful actions and/or inaction and the resulting Data Breach require Plaintiff and Class Members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiff and other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

CLASS ALLEGATIONS

127. Plaintiff brings this class action, individually and on behalf of the following Class:

All persons who were impacted by the Data Breach publicly announced by Defendant in August 2025 and received a Notice (the "Class").

128. Specifically excluded from the Class are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, principals, servants, partners, joint venturers, or entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

129. Plaintiff reserves the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

130. This action may be certified as a class action because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

131. Numerosity: The Class is so numerous that joinder of all Class Members is impracticable. Upon information and belief, the Class is comprised of thousands of members. The Class is sufficiently numerous to warrant certification.

132. Typicality of Claims: Plaintiff's claims are typical of those of other Class Members because Plaintiff, like the unnamed Class, had his Private Information compromised as a result of the Data Breach. Plaintiff is a member of the Class, and his claims are typical of the claims of the members of the Class. The harm suffered by Plaintiff is similar to that suffered by all other Class Members which was caused by the same misconduct by Defendant.

133. Adequacy of Representation: Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests antagonistic to, nor in conflict with, the Class. Plaintiff has retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

134. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members are relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful

conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

135. Predominant Common Questions: The claims of all Class Members present common questions of law or fact, which predominate over any questions affecting only individual Class Members, including:

- a. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- b. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- c. Whether Defendant's storage of Plaintiff's and Class Member's Private Information was done in a negligent manner;
- d. Whether Defendant had a duty to protect and safeguard Plaintiff's and Class Members' Private Information;
- e. Whether Defendant's conduct was negligent;
- f. Whether Defendant's conduct violated Plaintiff's and Class Members' privacy;
- g. Whether Defendant's conduct violated the statutes as set forth herein;
- h. Whether Defendant took sufficient steps to secure Plaintiff and Class Members Private Information;
- i. Whether Defendant was unjustly enriched; and
- j. The nature of relief, including damages and equitable relief, to which Plaintiff and Class Members are entitled.

136. Information concerning Defendant's policies is available from Defendant's records.

137. Plaintiff knows of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

138. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

139. Given that Defendant had not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION

COUNT I NEGLIGENCE

(On Behalf of Plaintiff and the Class)

140. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above as though fully set forth herein.

141. Plaintiff brings this claim individually and on behalf of the Class Members.

142. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

143. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Private Information.

144. Defendant had, and continues to have, a duty to timely disclose that Plaintiff's and Class Members' Private Information within its possession was compromised and precisely the types of information that were compromised.

145. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected individuals' Private Information.

146. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class Members. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

147. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

148. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information.

149. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Private Information;
- b. Failing to adequately monitor the security of its networks and systems; and

- c. Failing to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

150. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Defendant's possession.

151. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Private Information.

152. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

153. Defendant breached the duties set forth in 15 U.S.C. § 45, the FTC guidelines, the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. § 45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiff's and Class Members' Private Information. In violation of the FTC guidelines, *inter alia*, Defendant did not protect the Private Information it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of its networks' vulnerabilities; and failed to implement policies to correct security issues.

154. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would result in injury to Plaintiff and Class

Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

155. It was foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would result in injuries to Plaintiff and Class Members.

156. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised.

157. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiff and Class Members, their Private Information would not have been compromised.

158. As a result of Defendant's failure to timely notify Plaintiff and Class Members that their Private Information had been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

159. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiff and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

160. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above as though fully set forth herein.

161. Section 5 of the FTC Act, 15 U.S.C. 45, prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Plaintiff’s and Class Members’ Private Information. Various FTC publications and orders also form the basis of Defendant’s duty.

162. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiff’s and Class Members’ Private Information and by failing to comply with industry standards.

163. Defendant’s conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendant’s systems.

164. Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

165. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

166. As a result of Defendant’s negligence *per se*, Plaintiff and Class Members have been harmed and have suffered damages including, but not limited to: damages arising from

identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing, and correcting the current and future consequences of the Data Breach.

**COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)**

167. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above as though fully set forth herein.

168. Plaintiff and Class Members conferred a benefit upon Defendant by providing Defendant with their Private Information.

169. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff. Defendant also benefited from the receipt of Plaintiff's and Class Members' Private Information.

170. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the Class Members' Private Information because Defendant failed to adequately protect their Private Information. Plaintiff and the proposed Class would not have provided their Private Information to Defendant had they known Defendant would not adequately protect their Private Information.

171. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by it because of its misconduct and the Data Breach it caused.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

172. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above as though fully set forth herein.

173. Plaintiff and the Class provided and entrusted their Private Information to Defendant. Plaintiff and the Class provided their Private Information to Defendant as part of Defendant's regular business practices.

174. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen, in return for the business services provided by Defendant. Implied in these exchanges was a promise by Defendant to ensure that the Private Information of Plaintiff and Class Members in its possession was secure.

175. Pursuant to these implied contracts, Plaintiff and Class Members provided Defendant with their Private Information. In exchange, Defendant agreed to, among other things, and Plaintiff and the Class understood that Defendant would: (1) provide services to Plaintiff and Class Members'; (2) take reasonable measures to protect the security and confidentiality of Plaintiff and Class Members' Private Information; and (3) protect Plaintiff and Class Members' Private Information in compliance with federal and state laws and regulations and industry standards.

176. Implied in these exchanges was a promise by Defendant to ensure the Private Information of Plaintiff and Class Members in its possession was only used to provide the agreed-

upon reasons, and that Defendant would take adequate measures to protect Plaintiff and Class Members' Private Information.

177. A material term of this contract is a covenant by Defendant that it would take reasonable efforts to safeguard that information. Defendant breached this covenant by allowing Plaintiff and Class Members' Private Information to be accessed in the Data Breach.

178. Indeed, implicit in the agreement between Defendant and Plaintiff and Class Members was the obligation that both parties would maintain information confidentially and securely.

179. These exchanges constituted an agreement and meeting of the minds between the parties.

180. When the parties entered into an agreement, mutual assent occurred. Plaintiff and Class Members would not have disclosed their Private Information to Defendant but for the prospect of utilizing Defendant services. Conversely, Defendant presumably would not have taken Plaintiff and Class Members' Private Information if it did not intend to provide Plaintiff and Class Members with its services.

181. Defendant was therefore required to reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure and use.

182. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their Private Information.

183. Defendant breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff and Class Members' Private Information.

184. Defendant's failure to implement adequate measures to protect the Private Information of Plaintiff and Class Members violated the purpose of the agreement between the parties.

185. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiff and Class Members, Plaintiff and the Class Members suffered damages as described in detail above.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

- (a) For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representative of the Class and his counsel as Class Counsel;
- (b) For an order declaring that Defendant's conduct violates the laws referenced herein;
- (c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;
- (d) For damages in amounts to be determined by the Court and/or jury;
- (e) For an award of statutory damages or penalties to the extent available;
- (f) For pre-judgment interest on all amounts awarded;
- (g) For an order of restitution and all other forms of monetary relief; and
- (h) Such other and further relief as the Court deems necessary and appropriate.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: September 8, 2025

/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

David K. Lietz*
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Ave., NW, Suite 440
Washington, DC 20015
Phone: 866.252.0878
dlietz@milberg.com

Attorneys for Plaintiff and the Proposed Class

*Motion to appear *pro hac vice* forthcoming