UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF OHIO

MASON FINK, *individually and on behalf of all others similarly situated*, Plaintiff, v. UNION HOME MORTGAGE CORP., Defendant.	Case No. **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Mason Fink, on behalf of himself and all others similarly situated, through undersigned counsel, brings this class action against Union Home Mortgage Corp. ("Defendant" or "UHM") and alleges, upon personal knowledge as to his own actions and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff Fink brings this class action lawsuit on behalf of himself and a class of persons impacted by Defendant's failure to safeguard, monitor, maintain and protect highly sensitive personal and financial information of its current and former customers, including but not limited to names, loan numbers, Social Security Numbers, driver's license or government-issued ID card numbers, and dates of birth ("PII" or "Private Information") of Plaintiff and other similarly

situated individuals ("the Class"), provided to UHM in connection with their use of Defendant's mortgage and lending services.

2. Defendant's data security failures allowed a targeted cyberattack in June 2025 in which an unauthorized third party gained access to UHM's data systems, thereby accessing and exfiltrating sensitive information containing PII of thousands of Defendant's customers (the "Data Breach").[1]

3. Defendant began informing its customers of the Data Breach on or around September 15, 2025 via mailed letters which disclosed that unauthorized access to its systems had occurred and that sensitive personal information had been compromised (the "Notice").

4. Defendant's Notice failed to adequately disclose the full scope of the breach, the specific vulnerabilities that led to the unauthorized access, whether the threat had been contained, or what specific measures were being taken to prevent future breaches.

5. Entities like UHM that provide mortgage and lending services and handle customers' sensitive PII owe a duty to those individuals to keep their PII safe and secure from unauthorized access and disclosure. This duty arises because it is foreseeable that the exposure of PII to unauthorized persons-especially cybercriminals with nefarious intentions-will result in harm to the affected individuals.

6. Plaintiff and Class Members now face a substantial and imminent risk of identity theft, financial fraud, unauthorized account access, and other personal, social, and financial harms that may persist for life.

7. As a direct and proximate result of UHM's deficient security practices, Plaintiff's and Class Members' PII is now in the hands of unauthorized parties.

[1] *See Notice of Data Security Incident*, attached as Exhibit A.

8. Plaintiff and Class Members therefore suffer, and continue to face, ascertainable losses, including heightened risk of identity theft, out-of-pocket mitigation costs, lost time, diminished value of their PII, impending risk of fraud, identity theft, and dissemination of their data on the dark web.

9. Plaintiff and Class Members have already suffered concrete injuries in fact, including loss of data value, time and opportunity costs, and an uptick in spam calls, texts, and emails, and must now devote additional time, money, and effort to monitor accounts, secure credit files, and otherwise protect themselves.

10. On behalf of the Class, Plaintiff asserts claims for (i) Negligence; (ii) Breach of Implied Contract; (iii) Unjust Enrichment; (iv) Breach of Fiduciary Duty; and (v) Declaratory Judgment. Plaintiff seeks damages and injunctive relief, including Court-ordered implementation of industry-standard information-security measures, regular security audits, and long-term identity-theft-protection services to prevent future breaches.

PARTIES

11. Plaintiff Mason Fink is, and at all times relevant hereto was, a citizen of the State of Ohio, residing in Brecksville, Ohio. Plaintiff was a customer of Union Home Mortgage Corp. from 2021 through 2025.

12. Defendant Union Home Mortgage Corp. is an Ohio corporation with its principal place of business and corporate headquarters at 8241 Dow Circle, Strongsville, Ohio 44136.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d), because this is a class action in which: (a) there are at least 100 members in the proposed class; (b) members of the proposed class have a different citizenship from Defendant; and (c) the

claims of the proposed class members exceed $5,000,000 in the aggregate, exclusive of interest and costs. Plaintiff is a citizen of Ohio. Nevertheless, minimal diversity exists because members of the putative Class include individuals who are citizens of states other than Ohio, as Defendant regularly services mortgage loans and collects personal information from borrowers throughout the United States.

14. This Court has personal jurisdiction over Defendant because UHM maintains its principal place of business in this District, regularly conducts and solicits business in Ohio, is registered with the Secretary of State as a for profit corporation, and has committed tortious acts in this District.

15. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendant is deemed to reside in this District as a corporation subject to personal jurisdiction here at the time this action commenced. Venue is also proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in this District, including the data security failures that led to the breach and the decisions regarding data security practices made at Defendant's headquarters in Strongsville, Ohio.

COMMON FACTUAL ALLEGATIONS

A. UHM Collected, Maintained, and Stored PII.

16. Defendant is a mortgage company providing home loans, refinancing, and other financial services to thousands of customers throughout Ohio and nationwide. UHM operates branches in 44 states.[2]

[2] https://www.uhm.com/branches/

17. Plaintiff and Class Members are current and former customers who received mortgage or lending services from UHM, including conventional loans, refinancing, and other mortgage products.

18. In order to receive those services, customers—including Plaintiff and Class Members—were required to provide UHM with sensitive PII including their financial information, Social Security Numbers, dates of birth, driver's license or state identification numbers, passport numbers, loan account numbers, home addresses, and other personal data necessary for mortgage applications and loan processing.

19. Upon information and belief, UHM represented—through its privacy policy, customer agreements, and other disclosures—that it would maintain customers' PII in strict confidence and employ reasonable safeguards to protect it.

20. Given the highly sensitive nature of the information it collects for mortgage lending purposes, UHM is obligated to (i) keep customers' PII confidential; (ii) follow industry-standard data-security practices; (iii) inform customers of its data-security duties; (iv) comply with all applicable federal and state privacy laws, including mortgage industry regulations; (v) use or disclose the data only for legitimate mortgage lending and servicing purposes; and (vi) provide prompt notice of any unauthorized disclosure.

21. By obtaining and benefiting from Plaintiff's and Class Members' PII, UHM assumed legal and equitable duties to protect that data from unauthorized access or disclosure.

22. Without the submission of such data, UHM could not perform the mortgage origination, underwriting, and servicing operations it offers.

23. Plaintiff and Class Members reasonably relied on UHM to maintain their PII securely and to disclose it only as authorized. UHM ultimately failed to honor these duties.

B. UHM's Data Breach Exposed Highly Sensitive PII.

25. According to its Notice Letters, on June 25, 2025, UHM became aware of a data security incident it detected on its servers. After an unspecified amount of time, between the date it became aware and sent the notice letters, its investigation determined that an unauthorized actor accessed the UHM network and exfiltrated Plaintiff's and Class Members' Private Information.

26. On or around July 24, 2025 UHM began reporting to some State Attorneys General that information stolen in the Data Breach contained its customers' names, loan numbers, Social Security numbers, driver's license or government-issued ID card numbers, and/or dates of birth.

27. On August 26, 2025, UHM learned that Plaintiff's information was in the files stolen by cybercriminals.[3]

28. Defendant's Notice letter to Plaintiff and, upon information and good faith belief, Class Members, was dated September 15, 2025 – and therefore, ***Plaintiff's and Class members' PII was in the hands of cybercriminals for over 3 months before they were notified of UHM's Data Breach***. Time is of the essence when trying to protect against identity theft after a data breach, so early notification is critical.

29. The breach impacted tens of thousands of Defendant's customers nationwide.

30. The compromised information included highly sensitive data including:

a. Full names;

b. Social Security Numbers;

c. Home addresses;

[3] *Notice of Data Security Incident*, *supra* n. 1.

d. Dates of birth;

e. Driver's license or state identification numbers;

f. Passport numbers;

g. Loan account numbers;

h. Other personal information related to mortgage applications.

31. Defendant did not use reasonable security procedures and practices appropriate to the nature of the PII it was maintaining for Plaintiff and Class Members, causing the exposure of their PII.

32. Upon information and belief, the Private Information stored on UHM's network was not encrypted.

33. The unauthorized party accessed and acquired unencrypted files in Defendant's systems containing PII of Plaintiff and Class Members, which remains in the hands of cybercriminals.

34. Plaintiff reasonably believes his stolen Private Information is currently available for sale on the Dark Web because that is the modus operandi of cybercriminals who target businesses that collect highly sensitive Private Information.

35. Defendant has offered affected individuals only 24 months of complimentary credit monitoring and identity protection services, which is inadequate given the permanent nature of the compromised data, particularly Social Security Numbers, and the lifetime risk of identity theft.

36. UHM had obligations created by contract, industry standards, and common law to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

37. UHM could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting its equipment and computer files containing PII.

C. UHM Knew or Should Have Known of the Risk of a Data Breach

38. Defendant derives a substantial economic benefit from its mortgage and lending operations, which rely on hundreds of thousands of customer relationships through which Defendant requires, collects, and stores Plaintiff and Class Members' PII.

39. Defendant was well aware that the PII and financial information it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

40. Defendant also knew that a breach of its systems—and exposure of the information stored therein—would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised.

41. These risks are not merely theoretical; in recent years, numerous high-profile data breaches have occurred at financial institutions and mortgage companies such as Mr. Cooper (affecting 14.7 million customers in 2023), LoanDepot (16.9 million customers in 2024), and countless others in the mortgage and financial services industry.

42. PII has considerable value and constitutes an enticing and well-known target to hackers, who can easily sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."

43. Financial account information and loan account numbers, when combined with other PII such as Social Security Numbers, can be used to drain bank accounts, open new lines of credit, submit false mortgage applications, and engage in synthetic identity fraud.

44. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities.

45. In 2023, a record 3,205 data breaches occurred in the United States, resulting in about 349,221,481 sensitive records being exposed, a greater than 100% increase from 2019.

46. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years; for instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.

47. The mortgage and financial services industry has become a prime target for threat actors due to the comprehensive personal and financial data required for loan applications, including income verification, employment history, asset documentation, and credit information.

48. Additionally, mortgage lenders like UHM store a significant amount of confidential customer data that remains valuable long after loans are originated or serviced.

49. The breadth of data compromised in the Data Breach—including Social Security Numbers, driver's license numbers, passport numbers, and loan account information—makes the information particularly valuable to thieves and leaves Defendant's customers especially vulnerable to identity theft, mortgage fraud, and synthetic identity fraud.

50. A complete identity theft kit that includes mortgage-related financial information may be worth thousands of dollars on the black market, as it provides criminals with a comprehensive financial profile of victims.

51. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' PII to access accounts,

including, but not limited to, mortgage accounts, loan accounts, and other financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

52. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account, reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.

53. Identity thieves can use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information.

54. Social Security numbers, which were compromised in the Data Breach, are among the worst kind of information to have been stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

55. There may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is misused.

56. Even if stolen PII does not include all account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing.

57. Based on the value of its customers' PII to cybercriminals, Defendant certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

58. Despite the highly sensitive nature of the information that Defendant obtained, maintained, and stored and the prevalence of data breaches in the mortgage industry, Defendant inexplicably failed to take appropriate steps to safeguard the PII of Plaintiff and Class Members from being compromised.

D. UHM Knew or Should Have Known of the Risk Because Institutions in Possession of PII Get Targeted by Cybercriminals.

59. Given that Defendant was storing the PII of Plaintiff and Class Members and knew or should have known of the serious risk and harm caused by a data breach, Defendant was obligated to implement reasonable measures to prevent and detect cyber-attacks, such as those recommended by the Federal Trade Commission (the "FTC") and promoted by data security experts and other agencies.

60. That obligation stems from the foreseeable risk of a data breach given that Defendant collected, stored, and had access to a wealth of highly sensitive personal records and data and, additionally, because other highly publicized data breaches put Defendant on notice that the personal and sensitive data it stores might be targeted by cybercriminals.

61. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation and United States Secret Service have issued warnings to potential targets, so they are aware of, and prepared for, a potential attack.

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

63. Despite the abundance and availability of information regarding cybersecurity best practices and the prevalence of data breaches, Defendant inexplicably failed to adopt sufficient data security processes by, without limitation:

a. Failing to properly implement adequate access controls and monitoring systems;

b. Failing to ensure the proper monitoring and logging of network traffic;

c. Failing to ensure the proper monitoring and logging of file access and modifications;

d. Failing to ensure the proper training of employees as to cybersecurity best practices;

e. Failing to ensure fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiff and Class Members;

f. Failure to timely and accurately disclose that Plaintiff's and Class Members' PII had been improperly acquired or accessed;

g. Knowingly disregarding standard information security principles by allowing inadequate security measures;

h. Failing to provide adequate supervision and oversight of the PII with which it was entrusted.

64. Upon information and belief, Defendant further failed to ensure the proper implementation of sufficient processes to quickly detect and respond to data security incidents, to ensure the proper encryption of Plaintiff's and Class Members' PII, and to monitor user behavior and activity to identify possible threats.

65. Time is of the essence when PII is subject to unauthorized access and/or acquisition.

66. The disclosed, accessed, and/or acquired PII of Plaintiff and Class Members is, upon information and good faith belief, already available on the Dark Web.

67. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals.

68. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the publication of their PII onto the Dark Web.

69. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing sensitive personal information.

70. Despite the highly sensitive nature of the information that Defendant obtained, maintained, and stored and the prevalence of data breaches, Defendant inexplicably failed to take appropriate steps to safeguard the PII of Plaintiff and Class Members from being compromised.

71. The Data Breach itself, and information Defendant has disclosed about the breach to date, including its length, the need to remediate Defendant's cybersecurity, and the sensitive nature of the impacted data collectively demonstrate Defendant failed to implement reasonable measures to prevent cyber-attacks and exposure of the PII it oversaw.

E. Defendant Failed to Comply with FTC Guidelines.

72. The FTC recognizes that consumer data is a lucrative (and valuable) form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour underscored this point by reiterating that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[4]

[4] Pamela Jones Harbour, *Remarks Before FTC Exploring Privacy Roundtable* (Dec. 7, 2009), https://www.ftc.gov/news-events/news/speeches/remarks-ftc-exploring-privacy-roundtable (last visited Sept. 18, 2025).

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

74. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for business.

75. Those guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[5]

76. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[6]

77. The FTC has also issued, and regularly updates, guidelines for businesses to implement reasonable data security practices and incorporate security into all areas of the business.

78. According to the FTC, reasonable data security protocols require:

a. Encrypting the information stored on computer networks;

b. Retaining payment card information only as long as necessary;

---

[5] *Protecting Personal Information: A Guide for Business* (2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Sept. 18, 2025).

[6] *Start with Security: A Guide for Business* (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Sept. 18, 2025).

c. Properly disposing of personal information that is no longer needed or can be disposed pursuant to relevant state and federal laws;

d. Limiting administrative access to business systems;

e. Using industry approved activity;

f. Monitoring activity on networks to uncover unapproved activity;

g. Verifying that privacy and security features function properly;

h. Testing for common vulnerabilities; and

i. Updating and patching third-party software.[7]

79. The FTC cautions businesses that failure to protect PII and the resulting data breaches can destroy consumers' finances, credit history, and reputations, and can take time, money, and patience to resolve the effect.8 Indeed, the FTC treats the failure to implement reasonable and adequate data security measures-like Defendant failed to do here-as an unfair act prohibited by Section 5(a) of the FTC Act.

80. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act of practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

81. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

---

[7] *Id.*

[8] *See Taking Charge, What to Do if Your Identity is Stolen*, at 3 (Jan. 2012), https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen (last visited Sept. 18, 2025).

82. Defendant failed to properly implement basic data security practices.

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

84. Plaintiff alleges upon information and good faith belief, that Defendant was at all times fully aware of the obligation to protect the PII of their customers. Defendant was also aware of the significant repercussions that would result from their failure to do so.

F. UHM Failed to Comply with Industry Standards.

85. As shown above, experts studying cybersecurity routinely identify financial companies like Defendant as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

86. Several best practices have been identified that at a minimum should be implemented by companies like Defendant, including but not limited to educating all employees on cybersecurity best practices and measures; using strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; requiring multi-factor authentication; backup data; and limiting which employees can access sensitive data.

87. The United States Government and the United States Cybersecurity & Infrastructure Agency recommend several similar and supplemental measures to prevent and detect cyberattacks, including, but not limited to: implement an awareness and training program, enabling strong spam filters, scanning incoming and outgoing emails, configuring firewalls, automating anti-virus and anti-malware programs, managing privileged accounts, configuring access controls, disabling remote desktop protocol, and updating and patching computers.

88. Other best cybersecurity 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; training staff regarding critical points.

89. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2),[9] and the Center for Internet's Critical Security Controls[10] (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

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

91. UHM breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data.

92. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

---

[9] Nat'l Inst. of Standards & Tech., *Framework for Improving Critical Infrastructure Cybersecurity*(2018), https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf (last visited Sept. 18, 2025).

[10] *See The 18 CIS Critical Security Controls*, https://www.cisecurity.org/controls/cis-controls-list (last visited Sept. 18, 2025).

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect its customers' PII;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its employees with access to its computer systems employed reasonable security procedures;

e. Failing to detect unauthorized ingress into its systems;

f. Failing to implement and monitor reasonable network segmentation to detect unauthorized travel within its systems, including to and from areas containing the most sensitive data;

g. Failing to detect unauthorized exfiltration of the most sensitive data on its systems;

h. Failing to train its employees in the proper handling of emails containing PII and maintain adequate email security practices;

i. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and

j. Otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' PII.

93. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII. Accordingly, as outlined below, Plaintiff and Class Members now face actual fraud and identity theft as well as increased risk of fraud and identity theft. In addition, Plaintiff and Class Members lost the benefit of the bargain they made with Defendant.

G. Cyberattacks and Data Breaches Cause Disruption and Put Victims at an Increased Risk of Fraud and Identity Theft.

94. Cyberattacks and data breaches at companies like Defendant's are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

95. The United States Government Accountability Office released a report in 2007 regarding data breaches 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."[11]

96. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it.

97. They do this by selling the spoils of their cyberattacks on the black market to identify thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate piece of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim.

98. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique called "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

[11] *See* GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, at 2 (2007), https://www.gao.gov/new.items/d07737.pdf ("GAO Report") (last visited Sept. 18, 2025).

individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

99. The FTC recommends that identity theft 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 (and consider an extended fraud alert that lasts for 7 years if someone steal 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.[12]

100. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

101. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

102. In addition, thieves may obtain a job using the victim's Social Security Number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an issued victim's name.

103. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.[13]

[12] *See IdentityTheft.gov/Steps*, "https://www.identitytheft.gov/steps" (last visited Sept. 18, 2025).
[13] *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, 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).

104. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that 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.[14]

105. There may additionally be a substantial time lag—measured in years—between when harm occurs and when it is discovered, and also between when PII and/or financial information is stolen and when it is used.

106. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[15]

107. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black- market" for years.

108. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

109. Plaintiff and Class Members must vigilantly monitor their financial and other personal accounts for many years to come.

110. PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of the information and damage to victims may continue for years.

---

[14] *Id.*
[15] *The GAO Report*, *supra* n. 11, at 29.

111. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.16 Such fraud may go undetected until debt collection calls commence months, or even years, later.

112. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.

113. Each of these fraudulent activities is difficult to detect.

114. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud.

115. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

116. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

117. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse.

118. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[17]

119. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at the cybersecurity firm RedSeal, explained, "[c]ompared to credit

[16] *Identity Theft and Your Social Security Number* (2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Sept. 18, 2025).

[17] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back* (February 9, 2015), https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identtiy-theft (last visited Sept. 18, 2025).

card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[18]

120. For this reason, Defendant knew or should have known about these dangers and strengthened its data systems and data security measures accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

H. Plaintiff's and Class Members' Damages.

121. Upon information and good faith belief, Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

122. Plaintiff's and Class Members' PII was compromised in the Data Breach and is now in the hands of cybercriminals who accessed the data Defendant held within its systems. The PII exposed included the names, addresses, dates of birth, Social Security Numbers, financial account information, and other PII belonging to Defendant's current and former customers.

123. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

124. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach, valuable time Plaintiff and Class Members otherwise would have spent on other activities, including but not limited to work and/or recreation.

[18] Tim Greene, *Anthem hack: Personal Data stolen sells for 10x price of stolen credit card numbers* (February 6. 2015), https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Sept. 18, 2025).

125. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. This risk is particularly acute for minor children whose pristine credit histories and unused Social Security numbers make them prime targets for synthetic identity theft that may go undetected for years or even decades.

126. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

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

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

129. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members who are current or former employees or customers of Defendant's, or who otherwise submitted their data to Defendant, overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards.

130. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate data security practices to safeguard Plaintiff's and Class Members' PII.

131. As demonstrated by the Data Breach, Defendant failed to fund and provide adequate data security practices. Thus, Plaintiff and the Class Members who are current or former employees and customers of Defendant did not get what they paid for and agreed to.

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

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;
b. Purchasing credit monitoring and identity theft prevention;
c. Placing "freezes" and "alerts" with reporting agencies;
d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;
e. Contacting financial institutions and closing or modifying financial accounts; and
f. Closely reviewing and monitoring their bank accounts, credit reports, and medical insurance accounts, as well as alerts for identity fraud including their SSNs, for unauthorized activity for years to come.

133. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure

that the storage of data or documents containing PII is not accessible online or otherwise to unauthorized third parties.

134. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their PII—which contains the most intimate details about a person's life–may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

135. As a direct and proximate result of Defendant's actions and omissions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

REPRESENTATIVE PLAINTIFF'S EXPERIENCE

136. Plaintiff Mason Fink became a customer of UHM in approximately 2021, utilizing multiple financial services offered by Defendant throughout his membership including loan origination and servicing.

137. As a condition of obtaining services from Defendant, Plaintiff was required to provide his PII to Defendant, including his full name, Social Security Number, date of birth, driver's license number, address, and financial account information.

138. Defendant maintained Plaintiff Fink's PII in its systems at the time of the Data Breach.

139. On or about September 22, 2025, Plaintiff Fink received a Data Breach notification from Defendant, stating that his PII, including his Social Security Number and other sensitive information, may have been accessed or acquired as a result of the cyber incident.

140. Plaintiff is very careful about sharing his sensitive PII. He has trusted UHM with his personal and financial information based on their representations that they would safeguard

this information. Plaintiff would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

141. As a result of the Data Breach, Plaintiff Fink made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach, reviewing credit monitoring and identity theft protection services, monitoring his financial accounts for any unusual activity, and spending time reviewing his credit reports. This monitoring may need to continue for years to detect any fraudulent use of his information.

142. Plaintiff has spent significant time dealing with the Data Breach—valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

143. For example, Plaintiff has experienced several fraudulent attempts to initiate loans in his name in the past couple of months.

144. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) increased anxiety and stress about the misuse of his information; (vii) the continued and certainly increased risk to his PII, which remains in the hands of cybercriminals and may be sold on the dark web.

145. Given his relationship with UHM, Plaintiff placed particular trust in Defendant's ability and commitment to protect his information, making the breach of this trust especially damaging.

146. As a result of the Data Breach, Plaintiff Fink anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

147. Plaintiff Fink has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

148. Plaintiff brings this action pursuant to Fed. R. Civ. Pr. 23 on behalf of himself and all others similarly situated.

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

> All individuals residing in the United States whose PII was compromised by the Data Breach (the "Class").

150. The following people are excluded from the Class: (i) any judge or magistrate presiding over this action and members of their families; (ii) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parent has a controlling interest, and its current or former officers and directors; (iii) persons who properly execute and file a timely request for exclusion from the Class; (iv) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (v) Plaintiff's counsel and Defendant's counsel; and (vi) the legal representatives, successors, and assigns of any such excluded persons.

151. Numerosity: The exact number of members of the Class is large enough to render individual joinder impracticable. Members of the Class can be easily identified through Defendant's records and objective criteria permitting self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other data breach class action controversies.

152. Typicality: Plaintiff's claims are typical of the claims of other members of the Class in that Plaintiff, and the members of the Class, sustained damages arising out of Defendant's Data Breach, wrongful conduct and misrepresentations, false statements, concealment, and unlawful practices, and Plaintiff and members of the Class sustained similar injuries and damages, as a result of Defendant's uniform illegal conduct.

153. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Class. Plaintiff has no interests that conflict with, or are antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff.

154. Commonality and Predominance: There are many questions of law and fact common to the claims of Plaintiff and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

a. Whether Defendant violated the laws asserted herein;

b. Whether Defendant had a duty to use reasonable care to safeguard Plaintiff's and Class Members' PII;

c. Whether Defendant breached the duty to use reasonable care to safeguard Plaintiff's and Class Members' PII;

d. Whether Defendant breached its contractual promises to safeguard Plaintiff's and Class Members' PII;

e. Whether Defendant knew or should have known about the inadequacies of its data security policies and system and the dangers associated with storing PII;

f. Whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiff's and Class Members' PII from unauthorized release and disclosure;

g. Whether the proper data security measures, policies, procedures, and protocols were in place and operational within Defendant's computer systems to safeguard and protect Plaintiff's and Class Members' PII from unauthorized release and disclosure;

h. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

i. Whether Defendant's method of informing Plaintiff and other members of the Class was unreasonable;

j. Whether Defendant's conduct was likely to deceive the public;

k. Whether Defendant is liable for negligence or gross negligence;

l. Whether Defendant's conduct, practices, statements, and representations about the Data Breach of the PII violated applicable state laws;

m. Whether Plaintiff and Class Members were injured as a proximate cause or result of the Data Breach;

n. Whether Plaintiff and members of the Class were damaged as a proximate cause of the Data Breach;

o. Whether Defendant's practices and representations related to the Data Breach breached implied contracts with Plaintiff and members of the Class;

p. What the proper measure of damages is; and

q. Whether Plaintiff and members of the Class are entitled to restitutionary, injunctive, declaratory, or other relief.

155. Superiority: This cause is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered, and uniformity of decisions ensured.

156. A class action is superior to individual litigation because:

a. The amount of damages available to an individual plaintiff is insufficient to make litigation addressing Defendant's conduct economically feasible in the absence of the class action procedural device;

b. Individualized litigation would present a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system; and

c. The class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

157. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely and adequately notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard PII in its possession; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

158. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff & the Class)

159. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

160. Defendant required its customers, including Plaintiff and Class Members, to submit their PII to obtain financial services from Defendant.

161. By collecting and storing this data in its computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer system—and Plaintiff's and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

162. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, the personnel responsible for them, and its information technology partners adequately protected the PII.

163. Plaintiff and the Class are a well-defined, foreseeable, and probable group of customers that Defendant was aware, or should have been aware, could be injured by inadequate data security measures.

164. A large repository of highly valuable personal information is a foreseeable target for cybercriminals looking to steal and profit from that PII. Defendant knew or should have known that, given its repository of a host of PII for thousands of customers posed a significant risk of

being targeted for a data breach. Thus, Defendant had a duty to reasonably safeguard Plaintiff's and Class Members' data by implementing reasonable data security measures to protect against data breaches. The foreseeable harm to Plaintiff and the Class of inadequate data security created a duty to act reasonably and safeguard the PII.

165. After all, PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class Members. Thus, Defendant knew, or should have known, the importance of exercising reasonable care in handling the PII entrusted to them.

166. Defendant's duty of care to use reasonable security measures also arose as a result of the special relationship that existed between Defendant and its customers, which is recognized by laws and regulations, as well as common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

167. In addition, Defendant has a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.19

168. 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 PII.

[19] *See* 15 U.S.C. § 45.

169. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII. 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' PII;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to have in place mitigation policies and procedures;

d. Allowing unauthorized access to Plaintiff's and Class Members' PII;

e. Failing to detect in a timely manner that Plaintiff's and Class Members' PII had been compromised; and

f. Failing to timely notify Plaintiff and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

170. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class Members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite the known risk of data breaches, and allowing unauthorized access to Plaintiff's and Class Members' PII.

171. The failure of Defendant to comply with industry standards and federal regulations evidences Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII.

172. But for Defendant's wrongful and negligent breach of its duties to Plaintiff and Class Members, their PII would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the PII of Plaintiff and Class Members and all resulting damages.

173. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' PII would result in injury to Plaintiff and Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

174. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' PII would result in one or more types of injuries to Plaintiff and Class Members.

175. As a result of this misconduct by Defendant, the PII of Plaintiff and Class Members was compromised, placing them at a greater risk of identity theft and of their PII being disclosed to third parties without the consent of Plaintiff and the Class.

176. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

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

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff & the Class)

178. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

179. Defendant required Plaintiff and Class Members to provide and entrust their PII as a condition of obtaining services from Defendant and/or obtaining employment with Defendant.

180. Plaintiff and Class Members paid money to Defendant, directly and/or indirectly, in exchange for goods and/or services as well as Defendant's promise to protect their PII from unauthorized disclosure.

181. Defendant promised to comply with legal and industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

182. Implicit in the agreement between Defendant and Plaintiff and Class Members was the obligation that both parties would maintain the PII confidentially and securely.

183. Defendant had implied duties of good faith to ensure that the PII of Plaintiff and Class Members in their possession was used only as authorized.

184. Defendant had implied duties to protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses.

185. Additionally, Defendant implicitly promised to retain this PII only under conditions that kept such information secure and confidential.

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

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

188. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendant. Defendant did not. Plaintiff and Class Members would not have provided

their confidential PII to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their PII for uses other than obtaining benefits and services from Defendant.

189. Defendant breached the implied contracts with Plaintiff and Class Members by failing to safeguard and protect Plaintiff's and Class Members' PII; failing to provide timely and accurate notice to Plaintiff and Class Members that their PII was compromised as a result of the Data Breach; and violating industry standards as well as legal obligations that are necessarily incorporated into implied contracts between Plaintiff, Class Members, and Defendant.

190. Defendant's failures to meet these promises constitute breaches of the implied contracts.

191. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in Defendant providing goods and services to Plaintiff and Class Members that were of a diminished value.

192. Defendant's acts and omissions have materially affected the intended purpose of the implied contracts requiring Plaintiff and Class Members to provide their PII in exchange for services and employment benefits.

193. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the possibility of an illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non- economic harm.

194. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiff and Class Members are entitled to recover actual, consequential, and nominal damages.

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

195. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

196. This claim is pleaded solely in the alternative to Plaintiff's breach of implied contract claim in Count Two.

197. Plaintiff and Class Members conferred a monetary benefit on Defendant by using Defendant as a financial services provider. A portion of the proceeds of this benefit was intended to have been used by Defendant for data security measures to secure Plaintiff and Class Members' PII. Plaintiff and Class Members further conferred a benefit on Defendant by entrusting their PII to Defendant, from which Defendant derived profits.

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

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

200. Defendant acquired the monetary benefit and PII through inequitable means in that Defendant failed to disclose the inadequate security practices, as described herein, and failed to maintain adequate data security.

201. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to give their money—or disclosed their data— to Defendant.

202. Plaintiff and Class Members have no adequate remedy at law.

203. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered—and will continue to suffer—a host of injuries, including but not limited to: (1) actual identity theft; (2) the loss of the opportunity to determine how their PII is used; (3) the compromise, publication, and/or theft of their PII; (4) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (5) 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; (6) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their possession; and (7) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of Defendant's Data Breach.

204. The benefits that Defendant derived from Plaintiff and Class Members rightly belong to Plaintiff and Class Members. It would be inequitable under unjust enrichment principles for Defendant to be permitted to retain any of the profit or other benefits it derived from the unfair and unconscionable methods, acts, and data security practices alleged in this Complaint.

205. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds it received as a result of its conduct and the Data Breach alleged herein.

COUNT IV
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff & the Class)

206. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

207. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became a guardian of Plaintiff's and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class Members: (1) for the safeguarding of Plaintiff's and Class Members' PII; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and do store.

208. Defendant had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship with its current and former customers to keep their PII secure.

209. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give detailed notice of the Data Breach to Plaintiff and the Class in a reasonable and practicable period of time.

210. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' PII.

211. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

212. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PII.

213. As a direct and proximate result of Defendant's breaches of their fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (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; (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

214. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V
DECLARATORY JUDGMENT
28 U.S.C § 2201
(On Behalf of Plaintiff & the Class)

215. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

216. An actual controversy has arisen and now exists between Plaintiff and Class Members on the one hand, and Defendant on the other, concerning their respective rights and duties with respect to the Data Breach and Defendant's data security obligations going forward.

217. Plaintiff and Class Members contend that Defendant's data security measures were and remain inadequate and that Defendant has ongoing duties to implement and maintain reasonable safeguards to protect their PII that remains in Defendant's possession.

218. Plaintiff and Class Members further contend that Defendant has not adequately remediated the security vulnerabilities that led to the Data Breach and that their PII remains at imminent risk of further unauthorized access and disclosure.

219. Defendant has not provided adequate assurances that it has implemented sufficient security measures to prevent future breaches or that all copies of the exfiltrated data have been recovered or destroyed.

220. Pursuant to 28 U.S.C § 2201, this Court may declare the rights and legal relations of the parties to this action.

221. A judicial declaration is necessary and appropriate at this time so that the parties may ascertain their respective rights and duties with respect to:

a. Whether Defendant's current data security measures are adequate to protect Plaintiff's and Class Members' PII;

b. Whether Defendant must implement specific industry-standard security measures and protocols;

c. Whether Defendant must submit to regular third-party security audits and assessments;

d. Whether Defendant must provide ongoing credit monitoring and identity theft protection services to Class Members;

e. Whether Defendant must destroy or return any unnecessary PII in its possession; and

f. Whether Defendant must provide complete and transparent reporting regarding the Data Breach and remediation efforts.

222. Plaintiff and Class Members have no adequate remedy at law for Defendant's ongoing failure to implement adequate security measures, making declaratory relief appropriate.

223. Accordingly, Plaintiff and Class Members seek a declaration of their rights and Defendant's corresponding duties regarding data security practices and breach remediation measures.

DEMAND FOR RELIEF

WHEREFORE, Plaintiff Mason Fink, on behalf of himself and all persons similarly situated, prays for judgment in his favor and against Defendant Union Home Mortgage Corp., and respectfully requests that this Honorable Court enter an order:

A. certifying this action as a Class action and appointing Plaintiff as Class Representative and his counsel as Class Counsel;

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

C. granting equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the details of the Data Breach;

D. granting equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. requiring Defendant to pay for not less than five years of credit monitoring services for Plaintiff and the Class;

F. awarding actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

G. awarding punitive damages, as allowable by law;

H. awarding attorneys' fees and costs under the common fund doctrine, and any other applicable law;

I. awarding costs and any other expense, including expert witness fees, incurred by Plaintiff in connection with this action;

J. awarding pre- and post-judgment interest on any amounts awarded; and

K. all such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

DATED: September 30, 2025

Respectfully submitted,

By: */s/ Jared W. Connors*
Jared W. Connors (101451)
MEYER WILSON WERNING CO., LPA
305 W. Nationwide Blvd
Columbus, OH 43215
Telephone: (614) 224-6000
jconnors@meyerwilson.com

Elena A. Belov*
ALMEIDA LAW GROUP LLC
157 Columbus Avenue, 4th Floor
New York, New York 10023
Telephone: 347-395-5666
elena@almeidalawgroup.com

**Pro hac vice application forthcoming*

Attorneys for Plaintiff and the Putative Class