UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

MILREACE MALONE, individually and on behalf of all others similarly situated, Plaintiff, v. **UNDER ARMOUR, INC.** Defendant.	Case No. **DEMAND FOR JURY TRIAL** **CLASS ACTION COMPLAINT**

Plaintiff Milreace Malone ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendant Under Armour, Inc. ("Defendant") individually and on behalf of all others similarly situated, and allege, upon personal knowledge as to his own actions and his counsel's investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises out of the recent data breach ("Data Breach") involving Defendant that compromised Plaintiff's and Class Members' personally identifiable information ("PII" or "Private Information").

2. Founded in 1996 and headquartered in Baltimore, Maryland, Defendant is one of the largest athletic clothing producers in the United States.[1] Defendant generated $5.2 billion in revenue for fiscal year 2025.[2]

3. Upon information and belief, Plaintiff and Class Members were required to entrust Defendant with sensitive, non-public Private Information in connection with the services

[1] https://about.underarmour.com/en/our-company/history.html (last visited Nov. 24, 2025).
[2] https://about.underarmour.com/en/stories/press-releases/release.24836.html (last visited Nov. 24, 2025).

Defendant provides. Defendant retains this information for at least many years and even after the company relationship has ended.

4. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. On or around November 17, 2025, an unauthorized third party gained access to Defendant's inadequately secured systems and obtained files containing Plaintiff's and Class Members' Private Information (the "Data Breach").[3]

6. The notorious ransomware cybercriminal group Everest claimed responsibility for the Data Breach. Everest has a history of leaking data – in the past, it has attacked and leaked AT&T carrier website database with over half a million users' data, 1.5 million Dublin Airport passenger records, and internal Coca-Cola employee data. [4]

7. Everest published on its dark web leak site that it stole 343 GB of internal company data, employee information, along with personal data of millions from various countries. Everest also published sample data to prove the authenticity of their claims. Everest has issued a demand to Defendant to make contact with Everest within seven days, and Everest has published a countdown timer until "time runs out".[5]

8. Upon information and belief, Plaintiff's and Class Members' Private Information was compromised as a result of the Data Breach, including but not limited to, first names, email addresses, phone numbers, identifiers tied to user accounts, and other sensitive customer and employee data.

[3] https://hackread.com/everest-ransomware-under-armour-users-data/ (last visited Nov. 24, 2025)
[4] *Id.*
[5] *Id.*

9. Upon information and belief, Plaintiff's Private Information is available on the dark web as a result of the Data Breach.

10. To date, Defendant has yet to issue any public disclosure about the Data Breach.

11. Defendant failed to adequately protect Plaintiff's and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and their utter failure to protect Plaintiff's and Class Members' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk of identity theft and fraud to victims of the Data Breach will remain for their respective lifetimes.

12. In breaching its duties to properly safeguard Plaintiff's and Class Members' Private Information and give them timely, adequate notice of the Data Breach's occurrence, Defendant's conduct amounts to negligence and/or recklessness and violates federal and state statutes as well as its own internal privacy policies ("Privacy Policy").[6]

13. Plaintiff brings this action on behalf of himself, and 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; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free

[6] *Privacy Policy – Security*, Under Armour, https://privacy.underarmour.com/s/article/Security?language=en_US (last visited Nov. 24, 2025) ("We implement appropriate technical and organizational safeguards to protect against unauthorized or unlawful processing of personal data and against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. This includes such measures as establishment and implementation of internal management plan and periodic training for employees, controlling and periodically updating access to personal data in processing systems, encryption of certain data fields, and physical measures such as provision of external security and management of system server.")

of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

14. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the Private Information of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the Private Information of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

15. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (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) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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 Private Information.

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

17. Plaintiff is a natural resident and citizen of Baltimore, Maryland.

18. Defendant is a Maryland corporation maintaining its principal place of business at 101 Performance Drive, Baltimore, Maryland 21230.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

20. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is in this District, it regularly conducts business in this District, and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

21. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

FACTUAL ALLEGATIONS

Background of Defendant.

22. Defendant is one of the largest athletic clothing producers in the United States, generating $5.2 billion in revenue for fiscal year 2025.[7,8]

23. In connection with the services Defendant provides, Plaintiff and Class Members were required to provide Defendant with their sensitive and confidential Private Information.

[7] https://about.underarmour.com/en/our-company/history.html (last visited Nov. 24, 2025).
[8] https://about.underarmour.com/en/stories/press-releases/release.24836.html (last visited Nov. 24, 2025).

24. The information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class Members.

25. Upon information and belief, Defendant made promises and representations to Plaintiff and Class Members, that the Private Information collected from them would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it, including through its Privacy Policy.[9]

26. 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.

27. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

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

[9] *Privacy Policy – Security*, Under Armour, https://privacy.underarmour.com/s/article/Security?language=en_US (last visited Nov. 24, 2025)

Data Breaches Are Preventable.

29. Data breaches are preventable.[10] 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."[11] 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 . . . ."[12]

30. "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." [13]

31. 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 such risks.

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

33. Defendant failed to adequately protect Plaintiff's and Class Members' Private Information despite their knowledge of the risk of such a Data Breach occurring, and Defendant

---

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

[11] *Id.* at 17.

[12] *Id.* at 28.

[13] *Id.*

failed to take even basic measures to prevent the data breach—for example, Defendant failed to even encrypt or redact Plaintiff's and Class Members' highly sensitive data. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and their utter disregard for Class Members' privacy as well as Defendant's failure to fulfil their obligations to implement effective cyber-security practices and policies.

34. Defendant could have prevented this Data Breach by, among other things, properly encrypting, redacting, or otherwise protecting its equipment and computer files containing Private Information.

Value of Personally Identifying Information.

35. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[14] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employee-benefit management company or taxpayer identification number."[15]

36. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[16] For example, Personal Information can be sold at a price

[14] 17 C.F.R. § 248.201 (2013).
[15] *Id.*
[16] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Nov. 24, 2025).

ranging from $40 to $200.[17] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[18]

37. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), 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.[19]

38. Plaintiff and Class Members now face years of constant surveillance of their personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

Defendant Fails to Comply with FTC Guidelines.

39. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which 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.

40. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal information that they keep; properly dispose of personal

[17] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Nov. 24, 2025).
[18] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Nov. 24, 2025).
[19] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Nov. 24, 2025).

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.[20]

41. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[21]

42. The FTC further recommends that companies not maintain Private 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.

43. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect sensitive data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential 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.

44. These FTC enforcement actions include actions against companies like Defendant's.

[20] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Nov. 24, 2025).
[21] *Id.*

45. 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 businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

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

47. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

48. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of Plaintiff and Class Members, Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

Defendant Fails to Comply with Industry Standards.

49. As noted above, experts studying cyber security routinely identify companies in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

50. Several best practices have been identified that, at a minimum, should be implemented by companies in possession of Private Information, like Defendant, including but not limited to: educating all Plaintiff and Class Members; 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 Plaintiff and Class Members can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

51. Other best cybersecurity practices that are standard in the media industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

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

53. These foregoing frameworks are existing and applicable industry standards in the industry safeguarding Plaintiff and Class Members' data, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Common Injuries and Damages.

54. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession

of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (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) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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 Private Information.

55. The unencrypted Private Information of Plaintiff and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

56. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Simply put, unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

57. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

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

59. 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 of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater harm – yet the resource and asset of time has been lost.

60. Plaintiff and Class Members suffered actual injury and damages in the form of lost time that they spent on mitigation activities in response to the Data Breach.

61. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, contacting credit bureaus to place freezes on their accounts, and monitoring their accounts for any indication of unauthorized activity, which may take years to detect. Accordingly, the Data Breach has caused Plaintiff and Class Members to suffer actual injury in the form of lost time—which cannot be recaptured—spent on mitigation activities.

62. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that 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."[22]

[22] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007),

63. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal 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, placing a credit freeze on their credit, and correcting their credit reports.[23]

64. And for those Class Members who 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."[4]

65. Private Information is a valuable property right.[24] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

66. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. 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.

---

https://www.gao.gov/new.items/d07737.pdf. (last visited Nov. 24, 2025).

[23] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited Nov. 24, 2025).

[24] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Nov. 24, 2025) ("GAO Report").

67. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

68. The fraudulent activity resulting from the Data Breach may not come to light for years.

69. Plaintiff and Class Members now face years of constant surveillance of their personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

70. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to, upon information and belief, thousands and possibly even millions of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data[25].

71. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

Future Costs of Credit and Identity Theft Monitoring is Reasonable and Necessary.

72. Given the type of targeted attack, the sophisticated criminal activity, and the type of Private Information involved in this case, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and

[25] https://hackread.com/everest-ransomware-under-armour-users-data/(last visited Nov. 24, 2025)

purchase by criminals intending to utilize the Private Information for identity theft crimes, which has already been evidenced by Everest ransomware gang publishing sample data they exfiltrated on its official dark web leak site.

73. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to provide their Private Information to Defendant, Plaintiff and Class Members understood and expected that Defendant would properly safeguard and protect their Private Information, when in fact, 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 they struck with Defendant.

Plaintiff's Experience

74. Plaintiff is a former employee of Defendant.

75. As a condition of employment with Defendant, Plaintiff was required to provide his Private Information to Defendant.

76. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff's Private Information in its system.

77. Plaintiff is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

78. Plaintiff provided his Private Information to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's Privacy Policy, as well as state and federal law.

79. Plaintiff reasonably understood that in exchange for providing Defendant with his Private Information, Defendant would employ adequate cybersecurity measures and protect his Private Information.

80. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring his accounts for any indication of unauthorized activity, which may take years to detect. Plaintiff has spent significant time on mitigation activities in response to the Data Breach—valuable time Plaintiff 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.

81. Subsequent to the Data Breach, Plaintiff has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) nominal damages; and (vii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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 Private Information.

82. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

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

84. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

CLASS ACTION ALLEGATIONS

86. Plaintiff brings this nationwide class action on behalf of himself, and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

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

> **Nationwide Class**: All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach (the "Class").

88. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

89. Plaintiff reserves the right to amend the definitions of the Class or Subclass or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

90. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

91. Numerosity. The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. Although the precise number of individuals is currently unknown to Plaintiff and exclusively in the possession of Defendant, upon information and belief, thousands, and possibly even millions of individuals were impacted[26]. The Class is apparently identifiable within Defendant's records.

92. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendant had respective duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had respective duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

[26] https://hackread.com/everest-ransomware-under-armour-users-data/ (last visited Nov. 24, 2025)

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

h. 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;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiff and Class Members are entitled to actual damages and/or nominal damages as a result of Defendant's wrongful conduct; and,

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

93. Typicality. Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

94. Policies Generally Applicable to the Class. This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

95. Adequacy. Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages he has suffered is typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

96. Superiority and Manageability. The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

97. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that

experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

98. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

99. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

100. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

101. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

102. Likewise, particular issues under Rule 23(c)(2) 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 notify the Plaintiff and the class 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 Private Information;

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 its Plaintiff and Class Members' Private Information; and,

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

CAUSES OF ACTION

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

103. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 102, as if fully set forth herein.

104. Defendant requires Plaintiff and Class Members to submit non-public Private Information in connection with the services it provides.

105. Defendant gathered and stored the Private Information of Plaintiff and Class Members as part of its ordinary course of business.

106. Plaintiff and Class Members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

107. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

108. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

109. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, 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.

110. 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, and the personnel responsible for them, adequately protected the Private Information.

111. 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. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, which was required in connection with the services Defendant provides.

112. 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.

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

114. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Plaintiff's and Class Members' Private Information it was no longer required to retain pursuant to regulations.

115. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

116. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

117. Defendant breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. 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 Class Members' Private Information;

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

c. Allowing unauthorized access to Class Members' Private Information;

d. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

e. Failing to remove Plaintiff's and Class Members' Private Information they were no longer required to retain pursuant to regulations, and;

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

118. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

119. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

120. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm the statute was intended to guard against.

121. The FTC has pursued 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 as that suffered by Plaintiff and the Class.

122. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

123. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach

of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches targeting companies in possession of Private Information.

124. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

125. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

126. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

127. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

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

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

130. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

131. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

132. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (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) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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 Private Information.

133. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

134. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

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

136. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and insecure manner.

137. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their 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 all Class Members.

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

138. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 102, as if fully set forth herein.

139. 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 Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

140. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Private Information and not complying with industry

standards. 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.

141. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se.*

142. Plaintiff and Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

143. 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.

144. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered or will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (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) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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 Private Information.

145. Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial.

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

146. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 102, as if fully set forth herein.

147. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have had their Private Information protected with adequate data security.

148. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' Private Information for business purposes.

149. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

150. Defendant acquired the Private Information through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

151. If Plaintiff and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would not have entrusted their Private Information to Defendant.

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

153. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

154. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

155. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (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) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up 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 Private Information.

156. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

157. Plaintiff and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

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

158. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 102, as if fully set forth herein.

159. Plaintiff and the Class entrusted their Private Information to Defendant in connection with the services Defendant provides. 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.

160. At the time Defendant acquired the Private Information of Plaintiff and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the Private Information and not take unjustified risks when storing the Private Information.

161. Implicit in the agreements between Plaintiff and Class Members and Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent

unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the Private Information only under conditions that kept such information secure and confidential.

162. Plaintiff and the Class would not have entrusted their Private Information to Defendant had they known that Defendant would make the Private Information internet-accessible, not encrypt sensitive data elements, and not delete the Private Information that Defendant no longer had a reasonable need to maintain it.

163. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

164. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

165. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse,; actual identity theft crimes, fraud, and abuse,; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; lost work time; and other economic and non-economic harm.

166. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages to be determined at trial.

COUNT V
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

167. Plaintiff re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 102, as if fully set forth herein.

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

169. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiff alleges Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

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

a. Defendant continues to owe a legal duty to employ reasonable data security to secure the Private Information it possesses, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

b. Defendant continues to breach its duty by failing to employ reasonable measures to secure Plaintiff's and Class Members' personal information; and

c. Defendant's breach of its legal duty continues to cause harm to Plaintiff and the Class.

171. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect Plaintiff's and Class Members' data.

172. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

173. The hardship to Plaintiff and the Class if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued.

174. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiff and his Counsel to represent the Class;

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

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws.

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to

promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xii. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves;

F. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

G. For an award of attorneys' fees and costs as allowed by law;

H. For prejudgment interest on all amounts awarded; and

I. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff, individually and on behalf of the Class, hereby demands a trial by jury on all claims so triable.

Dated: November 24, 2025

/s/ Leanna Loginov

Leanna A. Loginov
SHAMIS & GENTILE, P.A.
14 NE First Avenue, Suite 705
Miami, FL 33132
Telephone: 305-479-2299
lloginov@shamisgentile.com

Attorney for Plaintiff and Proposed Class Members

JS 44 (Rev. 04/21)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

MILREACE MALONE, individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff Baltimore County, MD
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Leanna Loginov, Esq., Shamis & Gentile, P.A., 14 NE 1st Ave, Suite 705 Miami, FL 33132, 305.479.2299

DEFENDANTS

UNDER ARMOUR, INC.

County of Residence of First Listed Defendant Baltimore County, MD
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ◉ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☑ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☑ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
☐ 110 Insurance	PERSONAL INJURY	PERSONAL INJURY	☐ 625 Drug Related Seizure of Property 21 USC 881	☐ 422 Appeal 28 USC 158	☐ 375 False Claims Act
☐ 120 Marine	☐ 310 Airplane	☐ 365 Personal Injury - Product Liability	☐ 690 Other	☐ 423 Withdrawal 28 USC 157	☐ 376 Qui Tam (31 USC 3729(a))
☐ 130 Miller Act	☐ 315 Airplane Product Liability	☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability		INTELLECTUAL PROPERTY RIGHTS	☐ 400 State Reapportionment
☐ 140 Negotiable Instrument	☐ 320 Assault, Libel & Slander	☐ 368 Asbestos Personal Injury Product Liability		☐ 820 Copyrights	☐ 410 Antitrust
☐ 150 Recovery of Overpayment & Enforcement of Judgment	☐ 330 Federal Employers' Liability	PERSONAL PROPERTY	LABOR	☐ 830 Patent	☐ 430 Banks and Banking
☐ 151 Medicare Act	☐ 340 Marine	☐ 370 Other Fraud	☐ 710 Fair Labor Standards Act	☐ 835 Patent - Abbreviated New Drug Application	☐ 450 Commerce
☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)	☐ 345 Marine Product Liability	☐ 371 Truth in Lending	☐ 720 Labor/Management Relations	☐ 840 Trademark	☐ 460 Deportation
☐ 153 Recovery of Overpayment of Veteran's Benefits	☐ 350 Motor Vehicle	☐ 380 Other Personal Property Damage	☐ 740 Railway Labor Act	☐ 880 Defend Trade Secrets Act of 2016	☐ 470 Racketeer Influenced and Corrupt Organizations
☐ 160 Stockholders' Suits	☐ 355 Motor Vehicle Product Liability	☐ 385 Property Damage Product Liability	☐ 751 Family and Medical Leave Act	SOCIAL SECURITY	☐ 480 Consumer Credit (15 USC 1681 or 1692)
◉ 190 Other Contract	☐ 360 Other Personal Injury		☐ 790 Other Labor Litigation	☐ 861 HIA (1395ff)	☐ 485 Telephone Consumer Protection Act
☐ 195 Contract Product Liability	☐ 362 Personal Injury - Medical Malpractice		☐ 791 Employee Retirement Income Security Act	☐ 862 Black Lung (923)	☐ 490 Cable/Sat TV
☐ 196 Franchise				☐ 863 DIWC/DIWW (405(g))	☐ 850 Securities/Commodities/ Exchange
				☐ 864 SSID Title XVI	☐ 890 Other Statutory Actions
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS	IMMIGRATION	☐ 865 RSI (405(g))	☐ 891 Agricultural Acts
☐ 210 Land Condemnation	☐ 440 Other Civil Rights	Habeas Corpus:	☐ 462 Naturalization Application		☐ 893 Environmental Matters
☐ 220 Foreclosure	☐ 441 Voting	☐ 463 Alien Detainee	☐ 465 Other Immigration Actions	FEDERAL TAX SUITS	☐ 895 Freedom of Information Act
☐ 230 Rent Lease & Ejectment	☐ 442 Employment	☐ 510 Motions to Vacate Sentence		☐ 870 Taxes (U.S. Plaintiff or Defendant)	☐ 896 Arbitration
☐ 240 Torts to Land	☐ 443 Housing/ Accommodations	☐ 530 General		☐ 871 IRS—Third Party 26 USC 7609	☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
☐ 245 Tort Product Liability	☐ 445 Amer. w/Disabilities - Employment	☐ 535 Death Penalty			☐ 950 Constitutionality of State Statutes
☐ 290 All Other Real Property	☐ 446 Amer. w/Disabilities - Other	Other:			
	☐ 448 Education	☐ 540 Mandamus & Other			
		☐ 550 Civil Rights			
		☐ 555 Prison Condition			
		☐ 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)(2)

Brief description of cause:
Data breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5,000,000

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE 11/2425

SIGNATURE OF ATTORNEY OF RECORD /s/ Leanna Loginov

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Maryland

MILREACE MALONE, individually and on behalf of all others similarly situated

Plaintiff(s)

v.

UNDER ARMOUR, INC.

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* UNDER ARMOUR, INC.
c/o CSC-LAWYERS INCORPORATING SERVICE COMPAN, as Registered Agent
7 ST. PAUL STREET
SUITE 820
BALTIMORE MD 21202

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: Leanna Loginov
Shamis & Gentile, P.A.
14 NE 1st Avenue, Suite 705
Miami, Florida 33132

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____
was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____
_____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____
_____ , a person of suitable age and discretion who resides there,
on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is
designated by law to accept service of process on behalf of *(name of organization)* _____
_____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

ClassAction.org
