UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
BALTIMORE DIVISION

ORVIN GANESH, on behalf of himself and all others similarly situated,

Plaintiff,

v.

UNDER ARMOUR, INC.,

Serve:

CSC-Lawyers Incorporating Service Company
7 St. Paul Street, Suite 820
Baltimore, MD 21202

Defendant.

Case No.

CLASS ACTION COMPLAINT

(1) Negligence;
(2) Negligence Per Se;
(3) Breach of Implied Contract;
(4) Unjust Enrichment;
(5) Invasion of Privacy; and
(6) Declaratory Judgment

JURY TRIAL DEMANDED

Plaintiff Orvin Ganesh ("Plaintiff"), by and through his attorneys, hereby brings this Class Action individually and on behalf of all others similarly situated (collectively, "Class members"), against Defendant Under Armour, Inc. ("Defendant"). Plaintiff complains and alleges the following upon personal knowledge as to himself and upon information and belief as to all other matters.

INTRODUCTION

1. This is a data breach class action against Defendant for its failure to adequately secure and safeguard confidential and sensitive information of Plaintiff and the Class held through the typical course of business.

2. Plaintiff and the proposed Class members bring this class action lawsuit on behalf of all persons who entrusted Defendant with sensitive Personally Identifiable Information ("PII"), including names, email addresses, phone numbers, consent statuses, language preferences,

purchase timestamps, product identifiers, prices, quantities, store preference records, location data for cities and regions, marketing campaign logs, deep link tracking entries, and identifiers tied to user accounts and transactions, that was exposed in a data breach that occurred upon information and belief in November 2025 (the "Data Breach" or "Breach").

3. Defendant Under Armour, Inc., is one of the largest sports apparel companies in the United States, with a yearly revenue of $4.6 billion as of 2025.[1]

4. Plaintiff is a customer of Defendant who has purchased merchandise from Defendant's stores.

5. Through their business transactions with Defendant, Plaintiff and the Class members were required to provide, and did provide, their PII to Defendant.

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

7. On or around November 17, 2025, the Everest ransomware group announced that it had stolen 343 GB of Defendant's internal company data, which included the personal data of millions of customers and employees from various countries.[2]

8. The group published sample data of PII to substantiate their claim. This sample data of PII included first names, email addresses, phone numbers, consent statuses, language preferences, purchase timestamps, product identifiers, prices, quantities, store preference records, location data for cities and regions, marketing campaign logs, deep link tracking entries, and

[1] Demi Sher, *Under Armour: Facts and Statistics*, Investing.com (Oct. 30, 2025), https://www.investing.com/academy/statistics/under-armour-facts/.
[2] Waqas, *Everest Ransomware Says It Stole Data of Millions of Under Armour Users*, HackRead (Nov. 17, 2025), https://hackread.com/everest-ransomware-under-armour-users-data/.

identifiers tied to user accounts and transactions.[3]

9. Upon information and belief, Plaintiff's and Class members' PII was compromised as a result of this Data Breach.

10. Defendant has not acknowledged the Data Breach or notified impacted individuals that their sensitive personal data has been exposed.

11. Defendant failed to take precautions designed to keep individuals' PII secure.

12. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiff and the Class, to keep their PII confidential, safe, secure, and protected from unauthorized disclosure or access.

13. Plaintiff and the Class have taken reasonable steps to maintain the confidentiality and security of their PII.

14. Plaintiff and the Class reasonably expected Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

15. Defendant, however, breached its numerous duties and obligations by failing to implement and maintain reasonable safeguards; failing to comply with industry-standard data security practices and laws and regulations governing data security; failing to properly train its employees on data security measures and protocols; failing to timely recognize and detect unauthorized third parties accessing its system and that substantial amounts of data had been compromised; and failing to timely notify the impacted Class.

16. By implementing and maintaining reasonable safeguards and complying with

[3] *Id.*

standard data security practices, Defendant could have prevented this Data Breach.

17. As a direct result of Defendant's Data Breach, Plaintiff's and the Class's PII has been exposed to cybercriminals and may already be offered for sale on the dark web, where it can be accessed and exploited to the detriment of Plaintiff and the Class. Plaintiff and the Class face a current and lifetime risk of identity theft or fraud as a direct result of the Data Breach.

18. The modern cyber-criminal can use the PII and other information stolen in cyber-attacks to assume a victim's identity when carrying out various crimes such as:

(i) obtaining and using a victim's credit history;

(ii) making financial transactions on their behalf and without their knowledge or consent, including opening credit accounts in their name or taking out loans;

(iii) impersonating them in written communications, including mail, e-mail and/or text messaging;

(iv) stealing, applying for and/or using benefits intended for the victim; and

(v) committing illegal acts while impersonating their victim which, in turn, could incriminate the victim and lead to other legal ramifications.

19. Plaintiff's and Class members' PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect Plaintiff's and Class members' PII.

20. As a result of Defendant's failure to acknowledge the Breach, Plaintiff and the Class had no idea their PII had been compromised, and that they were, and continue to be, at significant and imminent risk of identity theft, fraud and various other forms of personal, social and financial harm. The risk will remain for their respective lifetimes because of Defendant's negligence.

21. Plaintiff brings this action on behalf of all persons whose PII was compromised in the Data Breach as a direct consequence for Defendant's failure to:

(i) adequately protect individuals' PII entrusted to it;

(ii) warn individuals of its inadequate information security practices; and

(iii) effectively monitor its websites and platforms for security vulnerabilities and incidents.

22. Defendant's conduct amounts to negligence and violates state and federal statutes and guidelines.

23. As a result of the Data Breach, Plaintiff and the Class suffered ascertainable losses, including but not limited to, a loss of privacy. These injuries include:

(i) the invasion of privacy;

(ii) the compromise, disclosure, theft, and imminent unauthorized use of Plaintiff's and the Class's PII;

(iii) emotional distress, fear, anxiety, nuisance and annoyance related to the theft and compromise of their PII;

(iv) lost or diminished inherent value of PII;

(v) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII;

(vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time or wages; and

(vii) the continued and increased risk to their PII, which remains available on the dark web for individuals to access and abuse and 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 of Plaintiff and the Class.

24. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose PII was compromised and stolen as a result of the Data Breach and remains at risk due to inadequate data security practices employed by Defendant.

25. Plaintiff, on behalf of himself and all other Class members whose PII was exposed in the Data Breach, asserts claims for negligence, negligence *per se*, breach of fiduciary duty, breach of implied contract, unjust enrichment, and invasion of privacy, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

26. Plaintiff Orvin Ganesh is a natural person and citizen of Texas.

27. Defendant Under Armour, Inc., is a corporation with its principal place of business located at 1020 Hull Street, Baltimore, Maryland 21230.

JURISDICTION AND VENUE

28. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d), and the amount in controversy exceeds the $5,000,000 jurisdictional minimum of the Class Action Fairness Act, exclusive of interest and costs, and there are numerous Class members who are citizens of states other than Defendant's states of citizenship.

29. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this jurisdiction, regularly conducts business in this jurisdiction,

and the acts and omissions giving rise to Plaintiff's claims emanated from within this jurisdiction.

30. Venue is proper in this jurisdiction because Defendant's principal place of business is in this jurisdiction and the acts and omissions giving rise to Plaintiff's claims emanated from within this jurisdiction.

FACTUAL ALLEGATIONS

Defendant Stores Consumer PII

31. Defendant Under Armour, Inc., is one of the largest sports apparel companies in the United States.

32. Defendant requires consumers to provide their sensitive personal information in order to use Defendant's services.[4]

33. Upon information and belief, the type of information that Defendant maintains includes names, dates of birth, email addresses, usernames, passwords, contact information, financial account information, purchase information, browser and device data, and information regarding individuals' fitness goals and experiences.[5]

34. Defendant's applicable privacy policy demonstrates that it is aware of its legal obligations to keep PII confidential and secure and indeed promises to do just that, stating: "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."[6]

35. Despite Defendant's representations about the privacy of consumers' information, it did not employ reasonable security measures to protect consumers' PII from unauthorized disclosure, as demonstrated throughout this Complaint.

36. Due to the sensitive nature of the information Defendant collects and maintains, Defendant is obligated to provide confidentiality and adequate security through its applicable

[4] *Privacy Policy: Personal Data We Collect*, Under Armour (Oct. 2022), https://privacy.underarmour.com/s/article/How-We-Use-Personal-Data?language=en_US.
[5] *Id.*
[6] *Privacy Policy: Security*, Under Armour (Oct. 2022), https://privacy.underarmour.com/s/article/Global-Privacy-Policy?language=en_US.

privacy policy, and otherwise in compliance with statutory privacy requirements.

37. Plaintiff and the Class members provided their PII to Defendant.

38. Plaintiff and Class members relied on Defendant to keep their sensitive PII confidential and secure, to use such information for business purposes only, and to make only authorized disclosures of this information.

The Data Breach

39. On or around November 17, 2025, the Everest ransomware group announced that it had stolen 343 GB of Defendant's internal company data, which included the personal data of millions of customers and employees from various countries.[7]

40. The group published sample data to substantiate their claim. This sample data revealed that the PII exposed included first names, email addresses, phone numbers, consent statuses, language preferences, purchase timestamps, product identifiers, prices, quantities, store preference records, location data for cities and regions, marketing campaign logs, deep link tracking entries, and identifiers tied to user accounts and transactions.[8]

41. Defendant has not acknowledged the Data Breach or notified impacted individuals that their sensitive personal data has been exposed.

42. Defendant's ongoing failure to notify Plaintiff and Class members that their PII was compromised places them at a higher risk that their information will be used towards illegal means since their information was vulnerable without their knowledge. Due to Defendants' failure to announce the Data Breach to consumers, Plaintiff and Class members were unable to take affirmative steps to mitigate their risks of fraud and/or identity theft from the unauthorized disclosure of their PII.

[7] Waqas, *supra* note 2.
[8] *Id.*

43. Defendant failed to take action to prevent the Data Breach by implementing data security measures to protect its network from unauthorized breach and thereby failed to protect consumers' PII.

44. Defendant further failed to timely detect the Data Breach until information was already accessed.

45. Upon information and belief, the cyberattack was targeted at Defendant due to its status as a large consumer retailer that collects, creates, and maintains customers' and employees' PII on its computer network and/or systems.

46. Plaintiff's and Class members' PII was compromised and acquired in the Data Breach.

47. Plaintiff further believes that their PII will continue to be available for purchase on the dark web, which is the *modus operandi* of cybercriminals.

48. Plaintiff and Class members now face a heightened and continued threat of identity theft and other types of criminal mischief resulting from the Data Breach. These consumers must now live the remainder of their lives under a threat that Defendant could have prevented.

Defendant Knew that PII is Valuable to Cybercriminals and Failed to Take Action to Prevent its Theft

49. At all relevant times, Defendant knew, or should have known, that Plaintiff's and Class members' PII in its possession was a target for cybercriminals.

50. Defendant should have been particularly aware of the threat cybercriminals pose, having been the target of a 2018 data breach that affected 150 million accounts on its MyFitnessPal platform.[9]

[9] Chloe Aiello, *Under Armour says data breach affected about 150 million MyFitnessPal accounts*, CNBC (Mar. 29, 2018), https://www.cnbc.com/2018/03/29/under-armour-stock-falls-after-company-admits-data-breach.html.

51. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII from cyberattacks.

52. By acquiring, collecting, and using Plaintiff's and Class members' PII, Defendant assumed legal and equitable duties created by the Federal Trade Commission Act, industry standards, contract, and statutory and common law to keep Plaintiff's and Class members' PII confidential, and to protect it from unauthorized access and disclosure.

53. Defendant certainly knew and understood that unprotected or exposed PII in its possession is valuable and highly sought after by criminals seeking to illegally monetize that PII through unauthorized access.

54. Indeed, personal data such as PII is a valuable property right, leading to the purchase of said data by American companies. American companies spent over $19 billion on acquiring personal data of consumers in 2018.[10]

55. Consumers place a high value on the privacy of their data. Studies confirmed that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[11] Recently, more consumers are exercising their Data Subject Access Rights and leaving providers over their data practices and policies.[12]

---

[10] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[11] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), available for download at: https://www.jstor.org/stable/23015560?seq=1.

[12] CISCO, *Cisco 2023 Consumer Privacy Survey* (April 2023), available at https://www.cisco.com/c/en/us/about/trust-center/consumer-privacy-survey.html?CCID=cc000742.

56. PII is also of high value to identity thieves, as evidenced by their practice of trading such private information on the black market or "dark web." PII is a measurable commodity on the black market.[13]

57. Companies like Defendant are aware that consumers value the privacy of their sensitive data such as PII and that cybercriminals continue to successfully target that data to obtain significant profits. As such, companies like Defendant remain on high alert and must act in accordance with their legal and equitable obligations to implement reasonable security measures to prevent targeted data attacks aimed at consumers' PII.

58. Armed with this knowledge, Defendant breached its duties by failing to implement and maintain reasonable security measures to protect Plaintiff's and Class members' PII from being stolen.

Theft of PII Has Grave and Lasting Consequences for Victims

59. Identity thieves use PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. According to Experian, one of the largest credit reporting companies in the world, identity theft can happen in many ways: fraudsters can obtain and sell personal data to other criminals, or use personal data to open a new credit card or loan, open a bank account and write bad checks, apply for government benefits, take over existing debit and credit accounts, withdraw funds, and even get medical procedures.[14]

60. The Federal Trade Commission ("FTC") also warns consumers about the type of

[13] *See, e.g.*, Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[14] Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Apr. 8, 2025), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

fraud that identity thieves use PII to achieve.[15] Criminals can 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 SSN to obtain government benefits, or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, 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 arrest warrant being issued in the victim's name.[16]

61. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a week to resolve issues stemming from identity theft and some need months to a year.[17]

62. Further complicating victims' ability to defend themselves from identity theft is the time lag between when PII is stolen, when it is used, and when a person discovers it has been used. On average, it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[18]

63. Plaintiff and Class members now live with their PII exposed in cyberspace and available to people willing to purchase and use the information for any number of improper purposes and crimes.

---

[15] *See What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER ADVICE, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last visited Dec. 12, 2025).
[16] *See Warning Signs of Identity Theft*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited Dec. 12, 2025).
[17] *2023 Consumer Impact Report*, Identity Theft Resource Center, available at https://www.idtheftcenter.org/wp-content/uploads/2023/08/ITRC_2023-Consumer-Impact-Report_Final-1.pdf.
[18] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), available at http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf

64. Plaintiff and Class members face constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class members are incurring and will continue to incur such damages, in addition to any fraudulent use of their PII.

Defendant Failed to Comply with Statutory Regulations

65. The Federal Trade Commission Act ("FTCA") prohibits Defendant from engaging in "unfair or deceptive acts or practices in or affecting commerce." *See* 15 U.S.C. § 45.

66. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that reflect the importance of implementing reasonable data security practices.

67. The FTC's publication, *Protecting Personal Information*, established cyber-security guidelines for businesses. The guidelines provide that businesses should take action to protect the personal information that they collect; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems.[19]

68. 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.[20]

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

[19] *Protecting Personal Information: A Guide for Business, Federal Trade Commission* (2016), available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.
[20] *Id.*

implemented reasonable security measures.

70. The FTC has the authority to bring enforcement actions against businesses for failing to protect PII adequately and reasonably under Section 5 of the FTCA, 15 U.S.C. § 45.

71. The orders that result from enforcement actions further clarify the measures businesses must take to meet their data security obligations.

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

73. Defendant was at all relevant times fully aware of its obligations to protect consumers' PII, and of the significant consequences that would result from its failure to do so.

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

75. Consequently, cybercriminals circumvented Defendant's lax security measures, resulting in the Data Breach.

Defendant Failed to Comply with Industry Standards

76. Industry standards for companies such as Defendant exist because of the high threat of cyberattacks that target the sensitive information that they collect and maintain.

77. These practices include, but are not limited to: educating and training employees about the risks of cyberattacks; creating strong passwords; implementing multi-layer security such as firewalls, anti-virus and malware software, encryption, and multi-factor authentication; backing up data; limiting employee access to sensitive data; setting up network firewalls; monitoring and limiting network ports; and monitoring and limiting access to physical security systems.

78. Defendant failed to meet the minimum standards of any of the following: 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.CM8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

79. Defendant's failure to implement the industry standards described herein resulted in the Data Breach and caused injury to Plaintiff and Class members.

Common Damages Sustained by Plaintiff and Class Members

80. For the reasons mentioned above, Plaintiff and all other Class members have suffered injury and damages directly attributable to Defendant's failure to implement and maintain adequate security measures, including, but not limited to: (i) a substantially increased risk of identity theft, justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) invasion of their privacy; (v) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face.

Plaintiff Orvin Ganesh's Experience

81. Plaintiff Orvin Ganesh resides in Texas.

82. Plaintiff is a customer of Defendant who has purchased merchandise from Defendant's stores.

83. In the course of conducting business with Defendant, Plaintiff provided Defendant with his PII.

84. On or around December 6, 2025, Plaintiff received an alert from CreditWise informing him that his email address was exposed in a breach of underarmour.com and found on the dark web.

85. Defendant never notified Plaintiff that the Breach occurred or that his PII had been exposed.

86. Since the Data Breach, Plaintiff has been required to spend valuable time monitoring his various accounts in an effort to detect and prevent any misuses of his PII, time he would not have had to spend but for the Data Breach.

87. Plaintiff has also recently noticed an increase in spam calls, texts, and emails. Spam calls have become so frequent that Plaintiff set up a call screening feature that requires individuals calling from unknown numbers to identify their reason for calling before they can get through to Plaintiff.

88. Plaintiff frequently conducts business via phone calls. Although Plaintiff believes the screening feature is necessary due to the number of spam calls he receives, it is also negatively impacting his business, as it deters some clients calling from unknown numbers from staying on the line long enough to speak to Plaintiff.

89. As a result of the Data Breach, Plaintiff suffered actual injury including, but not limited to: (i) a substantially increased risk of identity theft; (ii) improper disclosure of his PII; (iii) breach of the confidentiality of his PII; (iv) invasion of his privacy; (v) deprivation of the value of his PII, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft he faces and will continue to face.

90. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which is

amplified by the fact that key details about the Data Breach are still unknown, and Plaintiff's PII is still at risk of being stolen and used for fraudulent activity.

CLASS ALLEGATIONS

91. Plaintiff brings this class action individually and on behalf of all persons similarly situated, pursuant to 28 U.S.C. § 1332(d).

92. Plaintiff seeks certification of a Class as defined below and subject to further amendment:

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

93. Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

94. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

95. Numerosity. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. While the exact number of those affected by the Data Breach remains unknown, the Class size and the affected individuals' contact information is available from Defendant's business records.

96. Commonality. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members'

PII from unauthorized access and disclosure;

b. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII;

c. Whether Defendant breached its duties to protect Plaintiff's and Class members' PII;

d. Whether Defendant breached its fiduciary duty to Plaintiff and Class members;

e. When Defendant learned of the Data Breach;

f. Whether Defendant knew or should have known that its data security systems and monitoring procedures were deficient;

g. Whether hackers obtained Plaintiff's and Class members' data in the Data Breach;

h. Whether an implied contract existed between Class members and Defendant providing that Defendant would implement and maintain reasonable security measures to protect and secure Class members' PII from unauthorized access and disclosure;

i. Whether Defendant invaded Plaintiff's and Class members' privacy;

j. Whether Defendant was unjustly enriched;

k. Whether Plaintiff and Class members are entitled to injunctive relief and identity theft protection to redress the imminent harm they face due to the Data Breach; and

l. Whether Plaintiff and all other members of the Class are entitled to damages and the measure of such damages and relief.

97. Typicality. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like

all proposed members of the Class, had his PII compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

98. Adequacy of Representation. Plaintiff will fairly and adequately protect the interests of Class members. Plaintiff is an adequate representative of the Class in that he has no interests adverse to, or that conflict with, the Class he seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

99. Superiority. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and all other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class members to individually seek redress from Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

100. All members of the proposed Class are readily ascertainable. Defendant has access to the names, addresses, and/or email addresses of Class members affected by the Data Breach.

101. Finally, class certification is appropriate. Defendant engaged in a common course

of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of himself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(Plaintiff, on behalf of himself and the Class)

102. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

103. Defendant acquires consumers' PII in the ordinary course of its business.

104. Defendant collected, acquired, and stored Plaintiff's and Class members' PII.

105. Plaintiff and Class members entrusted Defendant with their private information and had the understanding that Defendant would safeguard their information.

106. Defendant had knowledge of the sensitivity of Plaintiff's and Class members' private information, and the consequences that would result from the unauthorized disclosure of such information. Defendant knew that large companies were the target of cyberattacks in the past, and that Plaintiff and Class members were the foreseeable and probable victims of any inadequate data security procedures.

107. It was therefore reasonably foreseeable that the failure to implement adequate data security procedures would result in injuries to Plaintiff and Class members.

108. Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their private information in its possession, custody, or control from the unauthorized disclosure of such information. Defendant also owed a duty to Plaintiff and Class members to notify them within a reasonable time of any breach to the security of their sensitive

and private information.

109. Defendant's duty to exercise reasonable care arises from several sources, including but not limited to common law, the FTCA, industry standards, and other statutory law.

110. Defendant breached its duty by failing to exercise reasonable care in safeguarding and protecting Plaintiff and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiff's and Class members' PII.

111. Defendant's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members caused their PII to be compromised in the Data Breach.

112. Plaintiff and Class members were in no position to protect their PII themselves.

113. But for Defendant's breach of the duties described herein, Plaintiff's and Class members' PII would not have been compromised.

114. There is a causal relationship between Defendant's failure to implement, control, direct, oversee, manage, monitor, and audit adequate data security procedures to protect consumers' PII and the harm suffered by Plaintiff and Class members.

115. Defendant's conduct caused the Data Breach, and as a direct and proximate result, Plaintiff and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) substantially increased risk of identity theft, justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) actual identity theft; (iii) improper disclosure of their PII; (iv) breach of the confidentiality of their PII; (v) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (vi) lost time and money incurred

to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

116. As a direct and proximate result of Defendant's wrongful conduct, Plaintiff and Class members have suffered and will continue to suffer other forms of injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

117. Plaintiff and Class members are entitled to damages incurred as a result of the Data Breach.

118. Defendant's negligent conduct is ongoing, in that it still holds Plaintiff's and Class members' PII in an unsafe and nonsecure manner.

119. Plaintiff and Class members are also entitled to injunctive relief in the form of requiring Defendant to strengthen its data security procedures and to provide credit monitoring to Class Members.

COUNT II
NEGLIGENCE PER SE
(Plaintiff, on behalf of himself and the Class)

120. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

121. Defendant's duties arise from Section 5 of the FTCA, 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendant, of failing to employ reasonable measures to protect and secure PII.

122. Defendant violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff and class members' PII and not complying with applicable industry standards.

Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

123. Defendant's violations of Section 5 of the FTCA constitute negligence *per se*.

124. Plaintiff and Class members are within the class of persons that Section 5 of the FTCA was intended to protect.

125. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA was intended to guard against.

126. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

127. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendant's violations of Section 5 of the FTCA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft, justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) actual identity theft; (iii) improper disclosure of their PII; (iv) breach of the confidentiality of their PII; (v) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they

face and will continue to face.

128. As a direct and proximate result of Defendant's wrongful conduct, Plaintiff and Class members have suffered and will continue to suffer other forms of injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

129. Plaintiff and Class members are entitled to damages incurred as a result of the Data Breach.

130. Plaintiff and Class members are also entitled to injunctive relief in the form of requiring Defendant to strengthen its data security procedures and to provide credit monitoring to Class members.

COUNT III
BREACH OF IMPLIED CONTRACT
(Plaintiff, on behalf of himself and the Class)

131. Plaintiff re-alleges and incorporates all foregoing paragraphs.

132. Plaintiff and the Class entrusted their PII with Defendant. In doing so, 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, compromised, or stolen.

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

134. Defendant breached the implied contract with Plaintiff and the Class by failing to safeguard and protect their PII, by failing to delete the PII of Plaintiff and the Class once their relationship ended, and by failing to provide timely and accurate notice to them that their PII was

compromised as a result of the Data Breach.

135. 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, resulting in monetary loss and economic harm; actual identify theft crimes, fraud, and abuse resulting in monetary loss and economic harm; 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; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic time that the Plaintiff and Class have not been compensated for.

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

COUNT IV
UNJUST ENRICHMENT
(Plaintiff, on behalf of himself and the Class)

137. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

138. This count is pleaded in the alternative to Plaintiff's breach of implied contract claim (Count IV).

139. Plaintiff and Class members conferred a monetary benefit upon Defendant in the form of their sensitive and private information.

140. In exchange, Plaintiff and Class members should have received from Defendant the benefit of its services and should have had their private information protected with adequate

data security procedures.

141. Defendant accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class members by acquiring and/or collecting their private information. Defendant appreciated and benefitted from the receipt of Plaintiff and class members' private information in that it used the private information and profited from the transactions in furtherance of its business.

142. Defendant acquired Plaintiff's and Class members' private information through inequitable means in that it failed to disclose the inadequate data security procedures previously alleged herein.

143. Defendant should not be permitted to retain the PII belonging to Plaintiff and Class members because Defendant failed to adequately implement the data privacy and security procedures for itself at the expense of Plaintiff and class members' safety and that were otherwise mandated by federal, state, and local laws and industry standards.

144. Defendant unjustly enriched itself by using the private information acquired from Plaintiff and Class members to further its business.

145. Notably, Defendant chose not to use any payments to enhance their data security procedures.

146. Had Plaintiff and Class members known of Defendant's inadequate security measures, they would not have provided their PII to Defendant to collect and maintain.

147. Under principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained from Plaintiff and Class members and should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

148. As a direct and proximate result of Defendant's wrongful conduct, Plaintiff and Class members have suffered and will continue to suffer other forms of injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

149. Plaintiff and Class members are entitled to equitable relief as a result of the Data Breach.

COUNT V
INVASION OF PRIVACY
(Plaintiff, on behalf of himself and the Class)

150. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

151. Defendant invaded Plaintiff's and Class members' right to privacy by allowing the unauthorized access to Plaintiff's and Class members' PII and by negligently maintaining the confidentiality of Plaintiff's and Class members' PII, as set forth in this Complaint. Defendant further invaded Plaintiff's and Class members' privacy by permitting third parties to access, disclose and publish Plaintiff's and Class members' PII online.

152. The intrusion was offensive and objectionable to Plaintiff and Class members, and to the reasonable person, in that Plaintiff's and Class members' PII was disclosed without prior written authorization of Plaintiff and other Class members.

153. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiff and the Class members provided and disclosed their PII to Defendant privately with an intention that their PII would be kept confidential and protected from unauthorized disclosure. It was reasonable for Plaintiff and the Class members to believe that such information would be kept private and would not be disclosed without their written

authorization.

154. As a direct and proximate result of Defendant's acts described throughout this Complaint, Plaintiff's and the Class members' PII was viewed, distributed, and used by persons without prior written authorization, and Plaintiff and the Class members suffered damages as described herein.

155. Defendant has committed oppression, fraud, or malice by permitting the unauthorized disclosure of Plaintiff's and the Class members' PII with a willful and conscious disregard of Plaintiff's and the Class members' right to privacy.

156. Plaintiff and Class members have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiff and the Class, and Defendant may freely treat Plaintiff's and Class members' PII with sub-standard and insufficient protections without intervention by this Court.

157. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause Plaintiff and the Class members great and irreparable injury in that the PII maintained by Defendant can be viewed, printed, distributed, and used by unauthorized persons.

COUNT VI
DECLARATORY JUDGMENT
(Plaintiff, on behalf of himself and the Class)

158. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

159. As previously alleged, Plaintiff and Class had an implied contract with Defendant that required Defendant to provide adequate security for the PII it collected. As previously alleged, Defendant owes duties of care to Plaintiff and Class members that require it to adequately

secure customer data.

160. Defendant still possesses PII information pertaining to Plaintiff and Class members.

161. Defendant has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems.

162. Accordingly, Defendant has not satisfied its legal duties to Plaintiff and Class members. In fact, now that Defendant's lax approach towards data security has become public, the PII data in its possession is more vulnerable than previously.

163. Actual harm from the ongoing threat of fraud and identity theft has arisen in the wake of the Data Breach.

164. Plaintiff, therefore, seeks a declaration that (a) Defendant's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. engaging 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;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting customer data by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access to other portions of Defendant systems;

e. purging, deleting, and destroying in a reasonable secure manner customer data not necessary for its provisions of services;

f. conducting regular database scanning and securing checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers and employees about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in their favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of himself and the Class, seeks appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit

monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

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

Dated: December 12, 2025

Respectfully submitted,

By: */s/ Jason S. Rathod*
Jason S. Rathod
(Maryland Federal Bar No. 18424)
MIGLIACCIO & RATHOD LLP
412 H Street NE, Ste. 302,
Washington, DC, 20002
Office: (202) 470-3520
jrathod@classlawdc.com

Beena M. McDonald*
Alex M. Kashurba*
Holly E. Jones*
CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
Telephone: (610) 642-8500
bmm@chimicles.com
amk@chimicles.com
hej@chimicles.com

**pro hac vice* to be submitted

Counsel for Plaintiff and the Proposed Class

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

Orvin Ganesh

(b) County of Residence of First Listed Plaintiff Denton Cty., TX
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Migliaccio & Rathod LLP, 412 H Street, NE, Ste. 302, Washington, DC 20002 202-470-3520

DEFENDANTS

Under Armour, Inc.

County of Residence of First Listed Defendant Baltimore Cty., 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
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

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. Section 1332(d)(2)(A)

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 $

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
December 12, 2025

SIGNATURE OF ATTORNEY OF RECORD
/s/ Jason Rathod

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

Orvin Ganesh

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.
1020 Hull Street
Baltimore, Maryland 21230.

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:

Jason Rathod, Esquire
Migliaccio & Rathod LLP
412 H Street, NE, Ste. 302
Washington, DC 20002

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: