UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

DAVID FREIFELD and STEVEN BOYLE, individually and on behalf of all others similarly situated, Plaintiffs, v. UNDER ARMOUR, INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs David Freifeld and Steven Boyle, ("Plaintiffs"), individually and on behalf of all others similarly situated ("Class Members"), upon personal knowledge of facts pertaining to them and on information and belief as to all other matters, by and through undersigned counsel, bring this Class Action Complaint against Defendant Under Armour, Inc. ("Under Armour" or "Defendant").

NATURE OF THE ACTION

1. Plaintiffs bring this class action individually and on behalf of all other individuals who had their sensitive personal information ("Personal Information") disclosed to unauthorized third parties during a data breach compromising Under Armour in November 2025 (the "Data Breach").

2. On November 17, 2025, the Everest ransomware gang ("Everest") announced that it had stolen 343 GB of Under Armour's internal company data, which included the personal data of millions. To prove the authenticity of its claim, Everest published a sample of the stolen data on its official dark web leak site.[1]

[1] Waqas, *Everest Ransomware Says It Stole Data of Millions of Under Armour Users*, HACKREAD

3. Under Armour has not yet publicly confirmed either the Data Breach or the nature of the data (e.g., names, addresses, and Social Security numbers) disclosed to, or accessed or acquired by, Everest.

4. According to Hackread, the leaked data includes "customer information and [] shipping history, along with other details, including email addresses, phone numbers, 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," as well as "customer data, including email addresses, first names, consent status, language preferences, and request timestamps."

5. Defendant was well aware of or should have known of its data security shortcomings. It collects and maintains sensitive Personal Information about its employees, consumers, and potential consumers, including Social Security numbers ("SSNs") and financial information.

6. Putting aside that large companies that collect sensitive Personal Information are routinely breached and that Under Armour is aware of this, Under Armour itself suffered a prior data breach in February 2018, which it disclosed the following month.[2]

7. Under Armour's 2018 data breach exposed the customer data of 150,000,000 users of the Under Armour-owned mobile application MyFitnessPal.[3] Moreover, Under Armour "admitted that some proportion of the exposed passwords were only hashed using a notoriously weak function called SHA-1, which has had known flaws for a decade and was further discredited

(Nov. 17, 2025), https://hackread.com/everest-ransomware-under-armour-users-data/.

[2] Luana Pascu, *My FitnessPal Hacked, 150 Million User Accounts Compromised*, BITDEFENDER (Mar. 30, 2018), https://www.bitdefender.com/en-us/blog/hotforsecurity/myfitnesspal-hacked-150-million-user-accounts-compromised/.

[3] *Id.*

by research findings [the previous] year."[4]

8. Nevertheless, Under Armour failed to make necessary changes to implement industry standard data privacy measures, again exposing its customers and, as here, its employees, to the risk of being impacted by a breach.

9. Defendant's failures to ensure that its servers and systems were adequately secure jeopardized the security of Plaintiffs' and Class Members' Personal Information, and exposed Plaintiffs and Class Members to fraud and identity theft or the serious risk of fraud and identity theft.

10. As a result of Defendant's conduct and the resulting Data Breach, Plaintiffs and Class Members' privacy has been invaded, their Personal Information is now in the hands of criminals, and they now face an imminent and ongoing risk of identity theft and fraud. Accordingly, these individuals now must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

PARTIES

11. Plaintiff David Freifeld is an adult citizen of the state of Illinois and resides in Lake County, Illinois. Plaintiff is a customer of Under Armour and made several purchases from Under Armour's website. Believing Under Armour would implement and maintain reasonable security and practices to protect its customers' Personal Information, Plaintiff Freifeld provided his Personal Information to Under Armour in connection with his purchases from Under Armour.

12. Plaintiff Freifeld expects to spend significat time dealing with the fallout of the Data Breach, including by enrolling in credit monitoring programs, changing passwords to numerous accounts, obtaining new debit/credit cards, and taking other actions in defense of the

[4] Lily Hay Newman, *The Under Armour Hack Was Even Worse Than It Had To Be*, WIRED (Mar. 30, 2018), https://www.wired.com/story/under-armour-myfitnesspal-hack-password-hashing/.

anticipated attacks on his identity, as a result of Defendant's failure to adequately secure Plaintiffs' Personal Information.

13. Plaintiff Steven Boyle is an adult citizen and resident of Washington, D.C. Plaintiff was an employee of Under Armour from 2015 to 2024. Believing Under Armour would implement and maintain reasonable security and practices to protect its employees' Personal Information, Plaintiff Boyle provided his Personal Information to Under Armour in connection with his employment with Under Armour.

14. Plaintiff Boyle expects to spend significant time dealing with the fallout of the Data Breach, including by enrolling in credit monitoring programs, changing passwords to numerous accounts, obtaining new debit/credit cards, and taking other actions in defense of the anticipated attacks on his identity, as a result of Defendant's failure to adequately secure Plaintiff Boyle's Personal Information.

15. Defendant Under Armour, Inc. is a corporation organized under the laws of the state of Maryland, with its principal place of business located in Baltimore, Maryland. Under Armour describes itself as "a leading inventor, marketer, and distributor of branded athletic performance apparel, footwear, and accessories."[5]

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00),

[5] Press Release: Under Armour Reports Second Quarter Fiscal 2026 Results; Provides Fiscal 2026 Outlook, UNDER ARMOUR (Nov. 6, 2025), https://about.underarmour.com/en/stories/press-releases/release.25226.html.

there are in excess of 100 Class Members, the action is a class action in which one or more Class Members are citizens of states different from Defendant, and Defendant is not a government entity.

17. The Court has personal jurisdiction over Defendant because Defendant is incorporated in Maryland, maintains its principal office in Baltimore, Maryland, operates in Maryland, conducts other significant business in Maryland, and otherwise has sufficient minimum contacts with and intentionally avails itself of the markets in Maryland.

18. Venue properly lies in this judicial district because, *inter alia,* Under Armour has a principal place of business in this district; Defendant transacts substantial business, has agents, and is otherwise located in this district; and a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this judicial district.

FACTUAL ALLEGATIONS

A. Under Armour Collects and Stores Personal Information

19. Under Armour routinely collects sensitive personally identifiable information ("PII") and/or protected health information ("PHI")—together, "Personal Information—from its employees, customers, users, and other individuals in relation to the employment, services, and products it offers.

20. In the U.S. Privacy Rights disclosure found on its website, Under Armour states that it may "collect sensitive personal data, including personal data that reveals a consumer's precise geolocation and personal data collected and analyzed concerning a consumer's health."[6]

21. The types of data Under Armour admits to collecting include, but are not limited to, a user's full name, addresses, phone numbers, email addresses, unique personal identifiers, IP addresses, financial details, credit or debit card numbers, demographic information, as well as

[6] U.S. State Privacy Rights, UNDER ARMOUR (updated July 10, 2024), https://privacy.underarmour.com/s/article/Residents-of-the-United-States?language=en_US.

specific and private physical characteristics such as sleep habits, nutritional intake, resting heart rate, and BMI.[7]

22. This is in addition to the sensitive Personal Information Under Armour collects from its employees as part of its onboarding process, which includes collecting SSNs, addresses, and financial details.

23. Defendant is and was aware of the sensitive nature of the Personal Information it collects, and it acknowledges the importance of data privacy. In the Privacy Policy disclosure on its website, Under Armour claims that it "implement[s] 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."[8]

24. Under Armour's Privacy Policy makes clear that it was aware of the need to safeguard the sensitive Personal Information entrusted to it by consumers when they purchased its products or subscribed to, downloaded, installed, or otherwise utilized its services, website(s), or mobile application(s).

25. Moreover, Under Armour's own 2018 data breach, in which 150 million Under Armour accounts associated with its MyFitnessPal mobile application were compromised, put Under Armour on notice of the potentially severe consequences that follow when such sensitive Personal Information is not adequately secured.

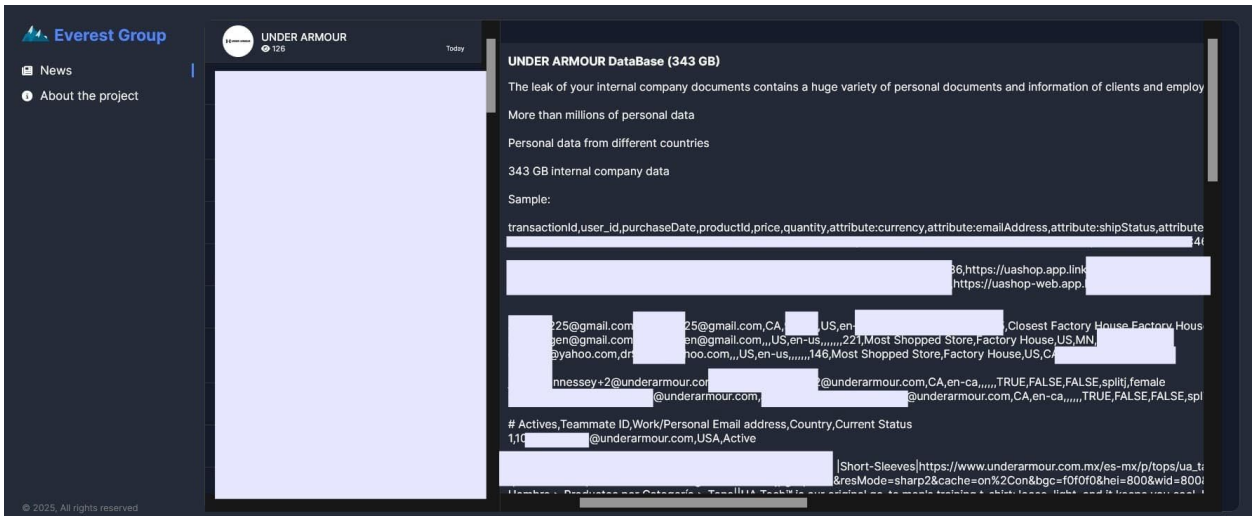
B. The Data Breach

26. In or about November 17, 2025, a threat actor claimed to have breached Under

[7] *Id.*
[8] Security, UNDER ARMOUR, https://privacy.underarmour.com/s/article/Security?language=en_US (last accessed Nov. 18, 2025).

Armour's systems, gaining access to Plaintiffs' and Class Members' sensitive Personal Information.

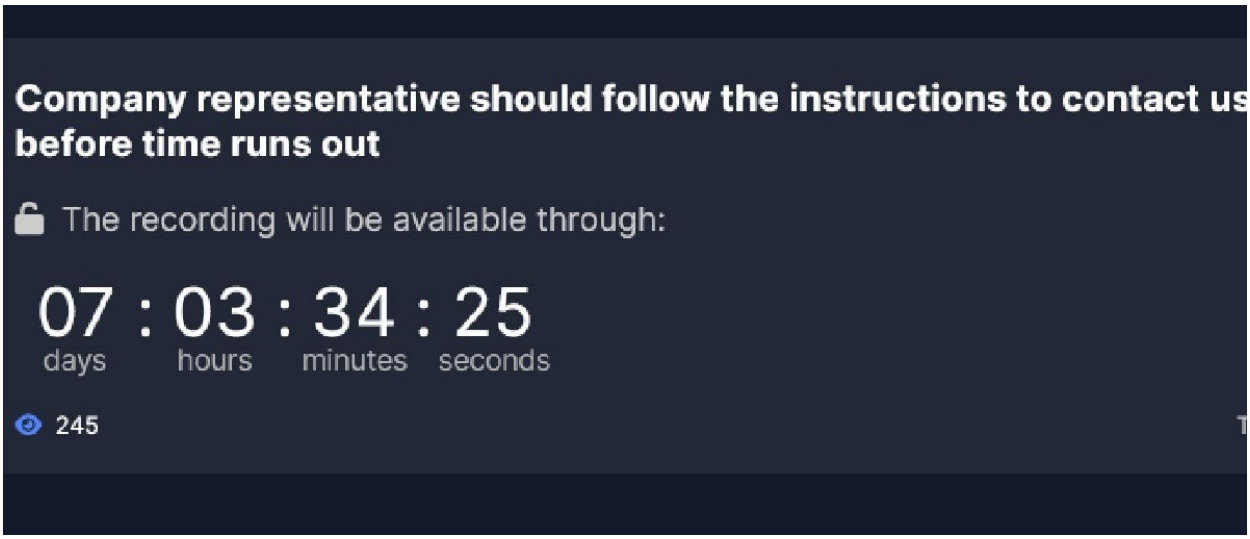
27. Everest, the threat actor, posted to its official website, which is only accessible via the "dark web," to announce its theft of "a huge variety of personal documents and information of clients and employees" from Under Armour[9]:



28. The posted sample contains, among other things, "customer information and their shopping history, along with other details, including email addresses, phone numbers, 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."[10]

[9] *Everest Ransomware Says It Stole Data of Millions of Under Armour Users*, n.1, *supra*.
[10] *Id.*

29. Making matters worse, Everest included a seven-day deadline for Under Armour to comply with its ransom demand, instructing Under Armour to follow specific steps to make contact with the ransomware group "before time runs out:"[11]



30. As of November 21, 2025, Under Armour has made no public acknowledgement of the Data Breach, nor has it yet responded to requests for comment from various publications.[12]

C. Impact of the Under Armour Data Breach

31. The actual extent and scope, and the impact, of the Data Breach on Under Armour's customers (or other affiliated persons) remains uncertain. Unfortunately for Plaintiffs and Class Members, the damage is already done because their sensitive Personal Information has been disclosed to unauthorized persons during the Data Breach.

[11] *Id.*

[12] *See, e.g.*, Stefanie Schappert, *Under Armour hit by ransomware, hackers claim "millions of personal data"*, CYBERNEWS (Nov. 17, 2025), https://cybernews.com/news/under-armour-allegedly-hit-by-ransomware-hackers-claim-millions-of-personal-data; Ellen Jennings-Trace, *Hackers claim to have hit Under Armour in massive data breach – here's what we know, and how you can stay safe*, TECH RADAR (Nov. 18, 2025), https://www.techradar.com/pro/security/hackers-claim-to-have-hit-under-armour-in-massive-data-breach.

32. Under Armour knew or should have known that its affected IT systems and/or servers are unsecure and do not meet industry standards for protecting highly sensitive customer Personal Information. On information and belief, Under Armour failed to timely make changes to its data security systems, privacy policies, and its IT systems and servers, exposing its customers' Personal Information to the risk of theft, identity theft, and fraud.

33. The harm caused to Plaintiffs and Class Members by the Data Breach has already been suffered. Even if companies, like Under Armour, that are impacted by ransomware attacks—and the Data Breach has been reported to be such an attack—pay the ransom, there is no guarantee that the criminals making the ransom demands will suddenly act honorably and destroy the sensitive Personal Information. In fact, there is no motivation for them to do so, given the burgeoning market for sensitive Personal Information on the dark web.

34. The Data Breach creates a heightened security concern for Plaintiffs and Class Members because their SSNs, financial information, and other sensitive information were potentially disclosed. Theft of SSNs creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of his SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

35. Given the highly sensitive nature of SSNs, theft of SSNs in combination with other personally identifying information (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. Per the United States Attorney General, Social Security numbers "can be an identity thief's most valuable piece of consumer information."[13] TIME quotes

[13] *Fact Sheet: The Work of the President's Identity Theft Task Force*, DEP'T OF JUSTICE, (Sept. 19, 2006), https://www.justice.gov/archive/opa/pr/2006/September/06_ag_636.html.

data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[14]

36. Under Armour had a duty to keep Plaintiffs' and Class Members' Personal Information confidential and to protect it from unauthorized disclosures. Plaintiffs and Class Members provided their Personal Information to Under Armour with the understanding that Under Armour would comply with its Privacy Policy and its obligations to keep such information confidential and secure from unauthorized disclosures.

37. Defendant's data security obligations were particularly important given the substantial increase in data breaches in recent years, including Under Armour's own 2018 data breach, which affected 150 million Under Armour accounts associated with its MyFitnessPal mobile application.

D. Theft of Personal Information Has Serious Consequences for Victims

38. Data breaches are by no means new and they should not be unexpected. Business Insider has noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers. . . . Many of them were caused by flaws in . . . systems either online or in stores."[15] It is well known amongst companies that store sensitive personally identifying information that sensitive Personal Information—like SSNs, financial information, tax information, etc.—is valuable and frequently targeted by criminals.

[14] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[15] Dennis Green et al., *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

39. These types of attacks should be anticipated by companies that store sensitive and personally identifying information, like Under Armour, and these companies must ensure that data privacy and security practices and protocols are adequate to protect against and prevent known and expected attacks.

40. Theft of Personal Information is serious. The Federal Trade Commission has warned consumers that identity thieves use Personal Information to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[16]

41. Indeed, with access to an individual's Personal Information, criminals can do more than simply empty a victim's bank account. They can also commit all manner of fraud, including: 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; obtain lending or lines of credit; 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.[17]

42. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a

[16] *See What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Nov. 24, 2025).
[17] *See Warning Signs of Identity Theft*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Nov. 24, 2025).

bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[18]

43. Personal Information is a valuable property right.[19] The value of sensitive personal information as a commodity is measurable.[20] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[21]

44. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web and the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen SSNs, financial information, driver's license numbers, and other Personal Information directly on various illegal websites making the information publicly available, often for a price. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

45. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal

[18] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[19] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

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

[21] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

information for a variety of crimes, including credit card fraud, tax fraud, phone or utilities fraud, and bank/finance fraud.

46. Consumers place a high value on the privacy of sensitive data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[22]

47. There may be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[23]

48. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Personal Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

49. 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 month to resolve issues stemming from identity theft and some need over a year.[24]

50. It is within this context that Plaintiffs and all other Class Members must now live with the knowledge that their Personal Information is forever in cyberspace and was taken by

[22] 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), https://www.jstor.org/stable/23015560?seq=1.
[23] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.
[24] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/.

people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

E. Under Armour Failed to Act in the Face of a Known Risk of a Data Breach

51. Despite the known risk of data breaches and the widespread publicity and industry alerts regarding other similar data breaches, Defendant failed to take reasonable steps to adequately protect the sensitive Personal Information in its possession, leaving its employees, customers, users, and other individuals exposed to risk of fraud and identity theft.

52. Under Armour is, and at all relevant times has been, aware that the sensitive Personal Information it handles and stores in connection with providing its services and products is highly sensitive. As a company that collects and utilizes highly sensitive and identifying information in connection with providing products, services and employment, Under Armour is aware of the importance of safeguarding that information and protecting its systems and products from security vulnerabilities.

53. Under Armour was aware, or should have been aware, of regulatory and industry guidance regarding data security, and was alerted to the risk associated with failing to ensure that Personal Information in its possession was adequately secured.

54. Despite the well-known risks of hackers and cybersecurity intrusions, Defendant failed to employ adequate data security measures in a meaningful way in order to prevent breaches, including the Data Breach.

55. The security flaws inherent to Defendant's IT systems or servers run afoul of industry best practices and standards. Had Defendant adequately protected and secured its servers or systems, and the sensitive Personal Information stored therein, it could have prevented the Data Breach.

56. Despite the fact that Under Armour was on notice of the very real possibility of data theft, including through its own prior data breach, it still failed to make necessary changes, and permitted a massive intrusion to occur that resulted in disclosure of Plaintiffs' and other Class Members' Personal Information to criminals.

57. Defendant permitted Class Members' Personal Information to be compromised and disclosed to criminals by failing to take reasonable steps against an obvious threat.

58. Industry experts are clear that a data breach is indicative of data security failures. Indeed, industry-leading research and advisory firm Aite Group has identified that: "If your data was stolen through a data breach that means you were somewhere out of compliance" with payment industry data security standards.[25]

59. As a result of the events detailed herein, Plaintiffs and Class Members suffered harm and loss of privacy, and will continue to suffer future harm, resulting from the Data Breach, including but not limited to: invasion of privacy; loss of privacy; loss of control over personal information and identities; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value and loss of possession and privacy of Personal Information; harm resulting from damaged credit scores and information; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized exposure of Personal Information.

60. Victims of the Data Breach are subject to an imminent and ongoing risk of harm, including identity theft and fraud.

[25] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 30, 2017), https://www.reuters.com/article/idUSKBN18M2BY/.

61. As a result of Under Armour's failure to ensure that its impacted systems and servers were protected and secured, the Data Breach occurred. As a result of the Data Breach, Plaintiffs' and Class Members' privacy has been invaded, their Personal Information is now in the hands of criminals, they face a substantially increased risk of identity theft and fraud, and they must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

CLASS ALLEGATIONS

62. Plaintiffs bring this action on behalf of themselves and the following Class pursuant to Federal Rule of Civil Procedure 23(a) and (b):

> All residents of the United States whose Personal Information was compromised as a result of the Under Armour Data Breach.

63. Excluded from the Class are: (1) any Judge presiding over this action, members of their immediate families, and Court Staff; and (2) Under Armour, its subsidiaries, parent companies, successors, predecessors, and any entity in which Under Armour, or its parents, have a controlling interest, and its current or former officers and directors.

64. **Numerosity**: While the precise number of Class Members has not yet been determined, members of the Class are so numerous that their individual joinder is impracticable, as the proposed Class appears to include millions of members who are geographically dispersed.

65. **Typicality**: Plaintiffs' claims are typical of Class Members' claims. Plaintiffs and all Class Members were injured through Defendant's uniform misconduct, and Plaintiffs' claims are identical to the claims of the Class Members they seek to represent. Accordingly, Plaintiffs' claims are typical of Class Members' claims.

66. **Adequacy**: Plaintiffs' interests are aligned with the Class Plaintiffs seek to represent, and Plaintiffs have retained counsel with significant experience prosecuting complex

class action cases, including cases involving alleged privacy and data security violations. Plaintiffs and undersigned counsel intend to prosecute this action vigorously. The Class's interests are well-represented by Plaintiffs and undersigned counsel.

67. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiffs' and other Class Members' claims. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class Members individually to effectively redress Defendant's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. 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.

68. **Commonality and Predominance:** The following questions common to all Class Members predominate over any potential questions affecting individual Class Members:

- whether Defendant engaged in the wrongful conduct alleged herein;
- whether Defendant's data security practices resulted in the disclosure of Plaintiffs' and other Class Members' Personal Information and the Data Breach;
- whether Defendant violated privacy rights and invaded Plaintiffs' and Class Members' privacy; and
- whether Plaintiffs and Class Members are entitled to damages, equitable relief,

or other relief and, if so, in what amount.

69. Given that Defendant engaged in a common course of conduct as to Plaintiffs and the Class, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

70. **Injunctive and Declaratory Relief:** Consistent with Fed. R. Civ. P. 23(b)(2), Defendant, through its conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

CAUSES OF ACTION

COUNT I
Negligence

71. Plaintiffs reallege and incorporate all previous factual allegations as though fully set forth herein.

72. Defendant was entrusted with, stored, and otherwise had access to the Personal Information of Plaintiffs and Class Members.

73. Defendant knew, or should have known, of the risks inherent to storing the Personal Information of Plaintiffs and Class Members, and to not ensuring that its servers and systems, and the Personal Information, were secure. These risks were reasonably foreseeable to Defendant, including because Defendant has previously experienced a data breach.

74. Defendant owed duties of care to Plaintiffs and Class Members whose Personal Information had been entrusted to it.

75. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate data security. Defendant had a duty to safeguard Plaintiffs' and Class Members' Personal Information and to ensure that their adequately protected Personal Information. Defendant breached this duty.

76. Under Armour's duty of care arises from its knowledge that its customers entrust it with highly sensitive Personal Information that Under Armour is required to, and represents that it will, handle securely. Indeed, on its website, Under Armour commits to data privacy in its Privacy Policy, including safeguarding sensitive Personal Information.

77. Only Under Armour was in a position to ensure that its systems, servers, and services were sufficient to protect against breaches and the harms that Plaintiffs and Class Members have now suffered.

78. A "special relationship" exists between Defendant, on the one hand, and Plaintiffs and Class Members, on the other hand. Defendant entered into a "special relationship" with Plaintiffs and Class Members by agreeing to accept, store, and have access to sensitive Personal Information provided by Plaintiffs and Class Members in connection with their purchase, subscription, and/or utilization of Under Armour's products and/or services.

79. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

80. Defendant acted with wanton disregard for the security of Plaintiffs' and Class Members' Personal Information.

81. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of duties. Defendant knew or should have known it was failing to meet these duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Personal Information.

82. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have been harmed and face an imminent and ongoing risk of harm.

83. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and

Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence Per Se

84. Plaintiffs reallege and incorporate all previous factual allegations as though fully set forth herein.

85. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Under Armour had a duty to provide adequate data security practices in connection with safeguarding Plaintiffs' and Class Members' Personal Information.

86. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Under Armour had a duty to provide adequate data security practices to safeguard Plaintiffs' and Class Members' Personal Information.

87. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801 *et seq.*) ("GLBA"), the Maryland Consumer Protection Act (Md. Code Ann., Com. Law §§ 13-101 *et seq*.) ("MCPA"), Maryland Personal Information Protection Act (Md. Code Ann., Com. Law §§ 14-3501 *et seq.*) ("MPIPA"), among other statutes, by failing to provide fair, reasonable, or adequate data security in connection with the sale of athletic products and services in order to safeguard Plaintiffs' and Class Members' Personal Information.

88. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

89. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

90. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of duties. Defendant knew or should have known that it

was failing to meet its duties, and that a breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Personal Information.

91. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and Class Members have been harmed and face an imminent and ongoing risk of harm.

92. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract

93. Plaintiffs reallege and incorporate all previous factual allegations as though fully set forth herein.

94. Under Armour sold or sells fitness apparel and services to Plaintiffs and Class members, or Plaintiffs and Class Members provided their Personal Information to Under Armour as employees, customers, or in some other capacity.

95. In connection with their business relationship, Plaintiffs and Class Members entered into implied contracts with Under Armour.

96. Pursuant to these implied contracts, Plaintiffs and Class Members provided Under Armour with their Personal Information. In exchange, Under Armour agreed, among other things: (1) to take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class Members' Personal Information; and (2) to protect Plaintiffs' and Class Members' Personal Information in compliance with federal and state laws and regulations and industry standards.

97. The protection of Personal Information was a material term of the implied contracts between Plaintiffs and Class Members, on the one hand, and Under Armour, on the other hand. Had Plaintiffs and Class Members known that Under Armour would not adequately protect its customers' Personal Information, they would not have done business with Under Armour.

98. Plaintiffs and Class Members performed their obligations under the implied contract when they provided Under Armour with their Personal Information.

99. Necessarily implicit in the agreements between Plaintiffs/Class Members and Under Armour was Under Armour's obligation to take reasonable steps to secure and safeguard Plaintiffs' and Class Members' Personal Information.

100. Under Armour breached its obligations under its implied contracts with Plaintiffs and Class Members by failing to implement and maintain reasonable security measures to protect their Personal Information.

101. Under Armour's breach of its obligations of its implied contracts with Plaintiffs and Class Members directly resulted in the Data Breach.

102. The damages sustained by Plaintiffs and Class Members as described above were the direct and proximate result of Under Armour's material breaches of its agreements.

103. Plaintiffs and other Class Members were damaged by Under Armour's breach of implied contracts because: (i) they have suffered actual harm or identity theft; (ii) they face a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their Personal Information was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their Personal Information has been breached; (v) they were deprived of the value of their Personal Information, for which there is a well-established national and international market; (vi) they were deprived of the benefit of their bargain; and/or (vii) they lost time and money incurred to mitigate and remediate the effects of the breach, including the increased risks of identity theft they face and will continue to face.

COUNT IV
Breach of Fiduciary Duty

104. Plaintiffs reallege and incorporate all previous factual allegations as though fully set forth herein.

105. A relationship existed between Plaintiffs and Class Members and Defendant in which Plaintiffs and Class Members put their trust in Defendant to protect the Personal Information of Plaintiffs and Class Members and Defendant accepted that trust.

106. Defendant breached the fiduciary duties that they owed to Plaintiffs and Class Members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the Personal Information of Plaintiffs and Class Members.

107. Defendant's breach of fiduciary duty was a legal cause of damage to Plaintiffs and Class Members.

108. But for Defendant's breach of fiduciary duty, the damage to Plaintiffs and Class Members would not have occurred.

109. Defendant's breach of fiduciary duty contributed substantially to producing the damage to Plaintiffs and Class Members.

110. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiffs are entitled to and demand actual, consequential, and nominal damages, and injunctive relief.

COUNT V
Violations of the Maryland Personal Information Protection Act
Maryland Code Ann., Com. Law §§ 14-3501 *et seq.*

111. Plaintiffs reallege and incorporate all previous factual allegations as though fully set forth herein.

112. This Count is brought pursuant to the MPIPA, which applies to Defendant because it is incorporated and headquartered in Maryland and/or engages in substantial business in Maryland, and because Defendant owns or licenses computerized data which includes Personal Information as defined under MPIPA. Md. Code Ann., Com. Law §§ 14-3501(b)(1)-(2).

113. Plaintiffs and Class Members are "individuals" or "consumers" as defined under MPIPA. Md. Code Ann., Com. Law §§ 14-3502(a), 14-3503.

114. Plaintiffs' and Class Members' compromised information includes Personal Information as defined under PIPA. Md. Code Ann., Com. Law § 14-3501(d).

115. Defendant violated MPIPA by:

a. failing to "protect personal information from unauthorized access, use, modification, or disclosure";

b. failing to "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned, maintained, or licensed"; and

c. failing to ensure its third-party service providers "implement and maintain reasonable procedures and practices[.]"

116. Defendant's failures and omissions were material because they were likely to induce consumers into purchasing, subscribing, or otherwise utilizing Defendant's products and/or services under the reasonable, but ultimately mistaken, assumption that Defendant would adequately safeguard their sensitive Personal Information.

117. Plaintiffs and the Class reasonably relied on Defendant's misrepresentations concerning its data privacy and security protocols.

118. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and

Class Members have been harmed and face an imminent and ongoing risk of harm.

119. On information and belief, Plaintiffs' Personal Information is now in the hands of cybercriminals and is in imminent danger of being published.

120. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT VI
Violation of the Maryland Consumer Protection Act
Maryland Code Ann., Com. Law §§ 13-101 *et seq*. ("MCPA")

121. Plaintiffs reallege and incorporate all previous factual allegations as though fully set forth herein.

122. This Count is brought pursuant the Maryland Consumer Protection Act, Md. Code Ann., Com. Law §§ 13-101 *et seq.* ("MCPA"), which applies to Defendant because it is incorporated and headquartered in Maryland and/or engages in substantial business in Maryland.

123. Plaintiffs and the Class are "consumers" as defined under the MCPA § 13-101(h).

124. Under Armour advertises, offers, or sells "consumer goods" and "consumer services" under the MCPA. Md. Code Ann., Com. Law § 13-101(d).

125. The MCPA prohibits "any unfair, abusive, or deceptive trade practice[.]" Md. Code Ann., Com. Law § 13-303.

126. Defendant violations of the MCPA represent direct and proximate causes of the Data Breach. These violations include Defendant's:

a. failure to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' Personal Information;

b. failure to identify foreseeable security risks relating to customer privacy, to remediate the identified security risks, and to adequately improve security and

private measures following previous cybersecurity incidents including Defendant's own major 2018 data breach;

c. failure to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801 *et seq*.;

d. omission, suppression, and concealment of the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' private personal information; and

e. omission, suppression, and concealment of the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801 *et seq*.

127. Defendant's failures and omissions were material because they were likely to induce consumers into purchasing, subscribing, or otherwise utilizing Defendant's products and/or services under the reasonable, but ultimately mistaken, assumption that Defendant would adequately safeguard their sensitive Personal Information.

128. Plaintiffs' and the Class reasonably relied on Defendant's misrepresentations concerning its data privacy and security protocols.

129. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have been harmed and face an imminent and ongoing risk of harm.

130. On information and belief, Plaintiffs' Personal Information is now in the hands of

cybercriminals and is in imminent danger of being published.

131. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT VII
Invasion of Privacy (Intrusion Upon Seclusion)

132. Plaintiffs reallege and incorporate all previous factual allegations as though fully set forth herein.

133. Plaintiffs and Class Members had a reasonable expectation of privacy in the Personal Information that Defendant disclosed without authorization.

134. By failing to keep Plaintiffs' and Class Members' Personal Information safe, knowingly employing inadequate data privacy policies and protocols, and disclosing Personal Information to unauthorized parties for unauthorized use, Defendant unlawfully invaded Plaintiffs' and Class Members' privacy by, *inter alia*:

a. intruding into Plaintiffs' and Class Members' private affairs in a manner that would be highly offensive to a reasonable person; and

b. invading Plaintiffs' and Class Members' privacy by improperly using their Personal Information properly obtained for a specific purpose for another purpose, or disclosing it to some third party;

c. failing to adequately secure Personal Information from disclosure to unauthorized persons;

d. enabling the disclosure of Plaintiffs' and Class Members' Personal Information without consent.

135. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' and Class Members' position would consider its actions highly offensive.

136. Defendant knew that its IT systems and servers were vulnerable to data breaches prior to the Data Breach.

137. Defendant invaded Plaintiffs' and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private affairs by disclosing their Personal Information to unauthorized persons without their informed, voluntary, affirmative, and clear consent.

138. As a proximate result of such unauthorized disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their Personal Information was unduly frustrated and thwarted. Defendant's conduct amounted to a serious invasion of Plaintiffs' and Class Members' protected privacy interests.

139. In failing to protect Plaintiffs' and Class Members' Personal Information, and in disclosing Plaintiffs' and Class Members' Personal Information, Defendant acted with malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private.

140. Plaintiffs seek injunctive relief on behalf of the Class, restitution, and all other damages available under this Count.

COUNT VIII
Unjust Enrichment

141. Plaintiffs reallege and incorporate all previous factual allegations as though fully set forth herein.

142. This claim is pleaded in the alternative to the implied contract claim.

143. Under Armour has profited and benefited from the monies or fees paid and the Personal Information provided by Plaintiffs and Class Members to receive services from Under Armour.

144. Under Armour has voluntarily accepted and retained these profits and benefits with full knowledge and awareness that, as a result of the misconduct and omissions described herein, Plaintiffs and Class Members did not receive services of the quality, nature, fitness, or value represented by Under Armour and that reasonable consumers expected.

145. Under Armour has been unjustly enriched by its withholding of and retention of these benefits, at the expense of Plaintiffs and Class Members.

146. Equity and justice militate against permitting Under Armour to retain these profits and benefits.

147. Plaintiffs and Class Members suffered injury as a direct and proximate result of Under Armour's unjust enrichment and seek an order directing Under Armour to disgorge these benefits and pay restitution to Plaintiffs and Class Members.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of the Class, by and through undersigned counsel, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiffs as class representatives and undersigned counsel as class counsel;

B. Award Plaintiffs and Class Members actual and statutory damages, punitive damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that Class Members have an effective remedy, including enjoining Defendant from continuing the unlawful practices as set forth above;

D. Award Plaintiffs and Class Members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiffs and Class Members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiffs and Class Members such other favorable relief as allowable under law or at equity.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: November 24, 2025

Respectfully submitted,

/s/ Steven M. Nathan
Steven M. Nathan (Bar ID # 30618)
HAUSFELD LLP
33 Whitehall Street, 14th Floor
New York, NY 10004
Tel: 646.357.1100
snathan@hausfeld.com

/s/ James J. Pizzirusso
James J. Pizzirusso (Bar ID # 20817)
HAUSFELD LLP
1201 17th Street N.W., Suite 600
Washington, D.C. 20036
Tel: 202.540.7200
jpizzirusso@hausfeld.com

/s/ Cyril V. Smith
Cyril V. Smith (Bar ID # 07332)
ZUCKERMAN SPAEDER LLP
100 East Pratt Street – Suite 2440
Baltimore, Maryland 21202
Tel: 410-332-0444
Fax: 410-659-0436
csmith@zuckerman.com

Tina Wolfson (pro hac vice forthcoming)
twolfson@ahdootwolfson.com
Sarper Unal (pro hac vice forthcoming)
sunal@ahdootwolfson.com
AHDOOT & WOLFSON, P.C.
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521

Telephone: (310) 474-9111
Facsimile: (310)474-8585

Attorneys for Plaintiffs and the Proposed Class

JS 44 (Rev. 03/24)

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

DAVID FREIFELD and STEVEN BOYLE, individually and on behalf of all others similarly situated,

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Steven M. Nathan; snathan@hausfeld.com
HAUSFELD LLP; Tel: 646.357.1100
33 Whitehall Street, 14th Floor, New York, NY 10004

DEFENDANTS

UNDER ARMOUR, INC.,

County of Residence of First Listed Defendant _____
(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
			IMMIGRATION	☐ 864 SSID Title XVI	☐ 890 Other Statutory Actions
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS	☐ 462 Naturalization Application	☐ 865 RSI (405(g))	☐ 891 Agricultural Acts
☐ 210 Land Condemnation	☐ 440 Other Civil Rights	**Habeas Corpus:**	☐ 465 Other Immigration Actions	FEDERAL TAX SUITS	☐ 893 Environmental Matters
☐ 220 Foreclosure	☐ 441 Voting	☐ 463 Alien Detainee		☐ 870 Taxes (U.S. Plaintiff or Defendant)	☐ 895 Freedom of Information Act
☐ 230 Rent Lease & Ejectment	☐ 442 Employment	☐ 510 Motions to Vacate Sentence		☐ 871 IRS—Third Party 26 USC 7609	☐ 896 Arbitration
☐ 240 Torts to Land	☐ 443 Housing/ Accommodations	☐ 530 General			☐ 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:** ☐ 540 Mandamus & Other ☐ 550 Civil Rights ☐ 555 Prison Condition ☐ 560 Civil Detainee - Conditions of Confinement			
	☐ 448 Education				

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)***:
Class Action Fairness Act, 28 U.S.C. §1332(d)

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 $ 5,000,000.00

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

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
Nov 24, 2025

SIGNATURE OF ATTORNEY OF RECORD
/s/ Steven M. Nathan

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 cases, if any. If there are related 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

DAVID FREIFELD and STEVEN BOYLE, 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.
101 PERFORMANCE DRIVE, BALTIMORE MD 21230
BY AND THROUGH ITS REGISTERED AGENT
CSC-LAWYERS INCORPORATING SERVICE COMPANY
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: Steven M. Nathan; snathan@hausfeld.com
HAUSFELD LLP
33 Whitehall Street, 14th Floor
New York, NY 10004
Tel: 646.357.1100

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: