

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

DAVID JOHNSTON, on behalf of himself and all
others similarly situated,

Plaintiff,

v.

NBCUNIVERSAL MEDIA LLC,

Defendant.

Case No. _____

CLASS ACTION

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

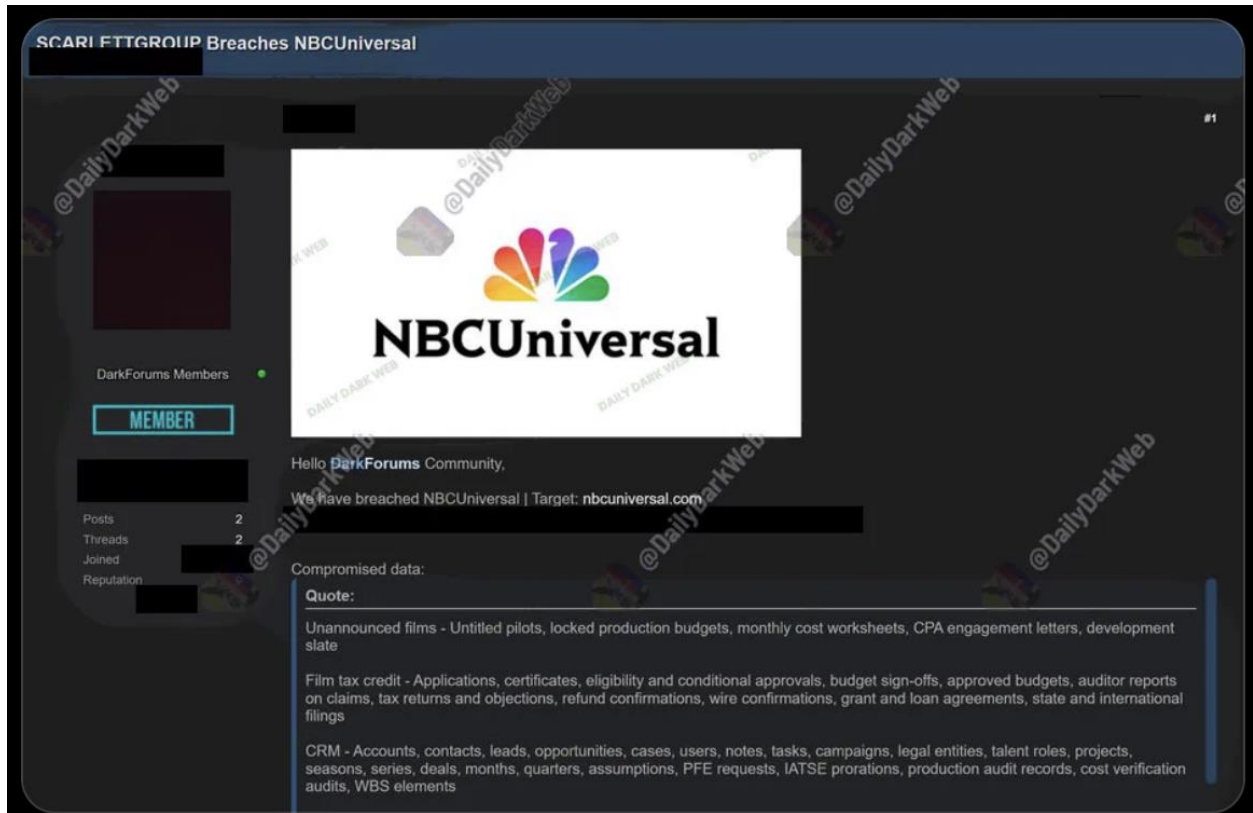
Plaintiff DAVID JOHNSTON (the “Plaintiff”), on behalf of himself and all others similarly situated, alleges the following Class Action Complaint (the “Action”) against the above-captioned Defendant, NBCUNIVERSAL MEDIA LLC (the “Defendant” or “NBC”) upon personal knowledge as to himself and his own actions, and upon information and belief, including the investigation of his counsel, as follows:

NATURE OF THE ACTION

1. NBC is an American mass media and entertainment conglomerate which is a subsidiary of Comcast and is headquartered at the iconic 30 Rockefeller Plaza in Midtown Manhattan, New York City, New York. Amongst its many lines of businesses, NBC is one of the largest television networks in the United States, owns a major film studio, and has numerous domestic digital streaming platforms, including Peacock. NBC also hosts consumer experiences and owns numerous theme parks.

2. In the process of providing media and entertainment goods and services to consumers, the NBC collects a significant amount of personally identifiable information (hereinafter, the “PII”) from its employees, including Plaintiff Johnston, who provide those services including, but not limited to their employee records (including their identifying information, payroll information, timecards, production files, talent roles, and other datapoints). This information was compromised as a result of a hacking and/or ransomware incident perpetrated by a cybercriminal organization called ScarlettGroup; additionally, other leaked information includes financial and tax documents, production records, Salesforce business records, commercial and operational information (collectively, the “Data Breach”). This information is

now accessible for viewing and misuse on the Dark Web, appearing available on a Dark Web forum:



3. The Data Breach unfolded as follows.

4. On October 18, 2026, ScarlettGroup posted the breached information on the above cybercrime forum. Then, the following day, on October 19, 2026, Cybernews published a report detailing the Data Breach after viewing samples of the compromised data. On or about October 23, 2026 or October 24, 2026, the above listed employee records were then made available for access, in combination with all of the other additional files as listed above. According to Cybernews, those files include: SAP general ledger reports, cost elements, financial records, CRM entries, Outlook emails, banking details, login records, source internet protocol addresses, access

histories, audit logs, and information about unannounced films, pilots, and future production schedules.¹

5. According to numerous news reports, ScarlettGroup attempted to negotiate with NBC before the release of the data from the Data Breach – but NBC apparently either did not negotiate proficiently to keep that data from being released or ScarlettGroup released the data anyway.

6. To compound matters, NBC's response to the Data Breach was woefully insufficient: (1) NBC still has not verified the Data Breach; (2) encompassed in the failure to verify the Data Breach – NBC has failed to disclose specifics of the cyberattack (i.e. how it happened) as well as specific remedial measures taken to ensure the protection of the PII still in the NBC's possession; and (3) victims and potential victims have been offered no remediation for the compromise of their information whatsoever. Each of these insufficiencies harm Plaintiff Johnston and the members of the putative Class and should be rectified.

7. As such, Plaintiff Johnston, on behalf of himself and all others similarly situated, brings this Action for actual damages, statutory damages, restitution, injunctive relief, disgorgement of profits and all other relief that this Court deems just and proper for breach of implied contract and negligence/negligence per se.

JURISDICTION AND VENUE

8. ***Subject Matter Jurisdiction.*** This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100

¹ Johnny Pelter, “NBCUniversal Data Breach Claim Remains Unverified,” CyPro (Online) (Oct. 19, 2026), at <https://cypro.co.uk/insights/cyber-bulletins/nbcuniversal-data-breach-claim-remains-unverified/>.

members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant, establishing the minimal diversity requirement of 28 U.S.C. § 1332(d).

9. ***Personal Jurisdiction.*** This Court has personal jurisdiction over Defendant NBC because NBC is both incorporated in New York and maintains its corporate headquarters in New York, New York.

10. ***Venue.*** Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the alleged wrongful conduct and events giving rise to the claims occurred in this District and because Defendant conducts significant business in this District, including maintaining its headquarters in this District.

PARTIES

Plaintiff David Johnston

11. Plaintiff Johnston is a natural person and is domiciled in Hampden County, Massachusetts. Plaintiff Johnston is a former employee of the Defendant, and, upon information and belief, had his PII compromised in the Data Breach as alleged herein.

Defendant NBCUniversal Media, LLC

12. Defendant is a New York limited liability company with its principal place of business located in New York, New York, at 30 Rockefeller Center.

FACTUAL ALLEGATIONS

Defendant's Business and Collection of PII

13. NBC is one of the cornerstones of American entertainment and media.

14. Dating back to 1950, NBC and Universal Television have had a partnership which focused primarily on television and cable channels. Today, NBC Universal is owned by Comcast as a subsidiary and has an annual revenue which exceeds \$39 billion. With over 35,000 employees

who work under the NBC banner, NBC is one of the largest entertainment and media employers in the United States.

15. Throughout the course of doing business, NBC collects a significant amount of personally identifiable information from its employees, including the PII contained in their employee records, as well as their name, financial account information, tax identification number, Social Security number, payment card information and driver's license number - as alleged herein.

16. In NBC's Privacy Policy, it admits that their privacy practices "[apply] to the NBCUniversal [services] throughout the world" with a responsibility to do so "as one of the world's leading media and entertainment companies." This is an obligation that it undertakes by contract as well as by statute, in tort, and consistent with industry standards.

Defendant's Data Breach

17. Between September and October of 2026, NBC suffered the Data Breach. This first became public knowledge on October 18, 2026 when ScarlettGroup, a cybercriminal hacking organization, posted on a Dark Web forum that they had compromised NBC's internal information.

18. ScarlettGroup posted on the forum a short description which invited NBC to negotiate the ransom associated with the corpus of data, including a description of the data as purported evidence.

19. On October 19, 2026, Cybernews, as well as other news organizations, were able to view stolen data samples shared by ScarlettGroup which included production plans, budget summaries, and tax credit applications. This sample of data also included material about projects which were scheduled to be released or produced from the present day through 2027.

20. On or about October 23, 2026 or October 24, 2026, ScarlettGroup released the entire corpus of compromised data onto aforementioned the Dark Web forum, which severely

compromised the data of Plaintiff Johnston and the Class members. According to online reporting, this information included employee records, financial and tax documents, production records, Salesforce business records, commercial and operational information.

21. As previously stated, NBC's response to the Data Breach remains and was woefully insufficient.

22. *First*, NBC has yet to confirm the Data Breach. This means that, for at least a week, if not more, NBC could have alerted employees to the fact that their PII might have been compromised – instead, NBC chose to sit on that information and allow valuable time to pass while members of the putative Class suffered the harms discussed herein.

23. *Next*, NBC has provided no restitution or remediation for victims of the Data Breach whatsoever. This means that, although it is well-documented that the harms from identity theft can affect a person for a lifetime, that NBC, a multi-billion dollar company, simply will not pay to provide victims of the Data Breach, the very employees who allowed the corporation to reach the levels that it has in terms of success and finances, with a very minimal ask – just to be compensated for NBC's failure to protect their information.

24. *Finally*, NBC has completely failed to disclose specifics of the cyberattack (i.e. how it happened) as well as specific remedial measures taken to ensure the protection of the PII still in the Defendant's possession. This means that NBC either does not know how the cyberattack occurred and is not taking any remedial measures to rectify their deficient cybersecurity apparatus, or that NBC has deliberately chosen not to inform the victims of the Data Breach of either how their PII was stolen or how it will be protected going forward. For victims of the Data Breach, all of this information remains unclear.

25. But what is clear from the Notice is that cybercriminals did, in fact, access and view Plaintiff Johnston and Class members' PII during the period in which the cybercriminals had unfettered access to Defendant's IT network, as that is the modus operandi of cybercriminals who commit such attacks.

26. Defendant did not implement or maintain adequate measures to protect its current and former employees' PII.

27. On information and belief, the PII compromised in the files accessed by hackers was not encrypted. This can be presumed given the hackers were able to access the data that was listed as compromised in the Notice of Data Event.

28. Moreover, the removal of PII from Defendant's system demonstrates that this cyberattack was targeted due to Defendant's status as a facility that houses sensitive PII.

29. Due to Defendant's incompetent security measures and its incompetent response to the Data Breach, Plaintiff Johnston and the Class members now face a present and substantial risk of fraud and identity theft and must deal with that threat forever.

30. Despite widespread knowledge of the dangers of identity theft and fraud associated with cyberattacks and unauthorized disclosure of PII, and despite Defendant's lucrative budget, Defendant provided unreasonably deficient protections prior to the Data Breach, including but not limited to a lack of security measures for storing and handling employees' PII and inadequate employee training regarding how to access, handle and safeguard this information.

31. Defendant failed to adequately adopt and train its employees on even the most basic of information security protocols, including: storing, locking encrypting and limiting access to current and former employees highly sensitive PII; implementing guidelines for accessing,

maintaining and communicating sensitive PII; and/or protecting sensitive PII by implementing protocols on how to utilize such information.

32. Defendant's failures caused the unpermitted disclosure of Plaintiff's and Class members' PII to an unauthorized third party and put Plaintiff and the Class at serious, immediate, and continuous risk of identity theft and fraud.

33. The Data Breach that exposed Plaintiff's and Class members' PII was caused by Defendant's violation of its obligations to abide by best practices and industry standards concerning its information security practices and processes.

34. Defendant failed to comply with security standards or to implement security measures that could have prevented or mitigated the Data Breach.

35. Additionally, Defendant failed to ensure that all personnel with access to its employees' PII were properly trained in retrieving, handling, using and distributing sensitive information.

The Breach Was Foreseeable

36. Defendant had weighty obligations created by industry standards, common law, and its own promises and representations made to Plaintiff and Class members to keep their PII confidential and to protect it from unauthorized access and disclosure.

37. Plaintiff and Class members provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

38. Defendant's data security obligations were particularly important given the substantial increase in ransomware attacks and/or data breaches in the entertainment and media industries preceding the date of the Data Breach.

39. Data breaches have become extremely widespread.

40. Defendant was aware of the risk of data breaches because such breaches have dominated the headlines in recent years.

41. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.

42. PII is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used in a variety of unlawful manners. PII can be used to distinguish, identify or trace an individual’s identity. This can be accomplished alone or in combination with other personal or identifying information that is connected or linked to an individual, such as the information compromised in this Data Breach.

43. Given the nature of the Data Breach, it is foreseeable that the compromised PII can be used by hackers and cybercriminals in a variety of different ways.

44. Cybercriminals who possess the Class members’ PII can readily obtain Class members’ tax returns or open fraudulent credit card accounts in the Class members’ names.

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

Defendant Failed to Follow FTC Guidelines and Industry Standards

46. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

47. According to the FTC, the need for data security should be factored into all business decision-making.

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

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

50. 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.

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

52. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer and employee data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

53. Defendant failed to properly implement some or all of these (and other) basic data security practices.

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

55. Defendant was at all times fully aware of its obligation to protect the PII of its employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

56. Additionally, and as detailed above, experts studying cyber security routinely identify consumer-facing (and employee hiring) businesses as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

57. Several best practices have been identified that, at a minimum, should be implemented by consumer goods and services providers such as Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; limiting which employees can access sensitive data.

58. Other best cybersecurity practices that are standard in the industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; and training staff regarding critical points.

59. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for

Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

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

Defendant's Breach

61. Defendant breached its obligations to Plaintiff and the Class members and was otherwise negligent and/or reckless because it failed to properly maintain and safeguard its computer systems, network and data.

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

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- b. Failing to adequately protect employees' PII;
- c. Failing to properly monitor its own data security systems for existing intrusions, brute-force attempts and clearing of event logs;
- d. Failing to apply all available and necessary security updates;
- e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;
- f. Failing to practice the principle of least-privilege and maintain credential hygiene;
Failing to avoid the use of domain-wide, admin-level service accounts;
- g. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords; and

- h. Failing to properly train and supervise employees in the proper handling of inbound emails;

63. As the result of allowing its computer systems to fall into dire need of security upgrading and its inadequate procedures for handling cybersecurity threats, Defendant negligently and unlawfully failed to safeguard Plaintiff's and the Class members' PII.

64. Accordingly, as outlined below, Plaintiff and Class members now face a substantial, increased, and immediate risk of fraud, identity theft, and the disclosure of their most sensitive and deeply personal information.

Data Breaches Are Disruptive and Harmful

65. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

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

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

68. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number.

69. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

70. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.¹¹

71. Theft of PII is gravely serious. PII is an extremely valuable property right.

72. Its value is axiomatic, considering the value of “big data” in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

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

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm. *See* GAO Report, at p. 29.

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

75. There is a strong probability that entire batches of information stolen in the Data Breach have been dumped on the black market and are yet to be dumped on the black market,

meaning Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the future.

76. Thus, Plaintiff and Class members must vigilantly monitor their financial accounts for many years to come.

Harm to Plaintiff

77. As a result of the Data Breach, Plaintiff Johnston made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff has already spent multiple hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on his other activities.

78. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

79. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

CLASS ALLEGATIONS

80. This Action is properly maintainable as a Class Action under Federal Rule of Civil Procedure 23. As such, Plaintiff brings this Action on behalf of himself and all similarly situated persons for the following Class defined as:

Class Definition. All individuals residing in the United States whose PII was compromised on the Data Breach which compromised Defendant's data during September of 2026.

(collectively, the "Class").

81. Excluded from the Classes are: Defendant and Defendant's subsidiaries, affiliates, officers and directors, and any entity in which the Defendant has a controlling interest; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

82. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

83. **Numerosity.** Defendant reports that the Data Breach compromised PII of as many as 35,000 current and former employees. Therefore, the members of the Class are so numerous that joinder of all members is impractical.

84. **Commonality.** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

- a. Whether Defendant unlawfully used, maintained, lost or disclosed Plaintiff's and Class members' PII;
- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

- d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- e. Whether Defendant owed a duty to Class members to safeguard their PII;
- f. Whether Defendant breached its duty to Class members to safeguard their PII;
- g. Whether computer hackers obtained Class members' PII in the Data Breach;
- h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- i. Whether Plaintiff and Class members suffered legally cognizable damages as a result of Defendant's misconduct;
- j. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;
- k. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and
- l. Whether Plaintiff and Class members are entitled to damages, civil penalties, punitive damages, equitable relief and/or injunctive relief.

85. **Typicality.** Plaintiff's claims are typical of those of other Class members because Plaintiff's PII, like that of every other Class member, was compromised by the Data Breach. Further, Plaintiff, like all Class members, was injured by Defendant's uniform conduct. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of other Class members arise from the same operative facts and are based on the same legal theories.

86. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Class in that she has no disabling or disqualifying conflicts of interest that would be antagonistic to those of the other members of the Class. The damages and infringement of rights Plaintiff suffered are typical of other Class members, and Plaintiff seeks no

relief that is antagonistic or adverse to the members of the Class. Plaintiff has retained counsel experienced in complex consumer class action litigation, including, but not limited to, data breach class action litigation, and Plaintiff intends to prosecute this action vigorously.

87. **Superiority of Class Action.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy, as the pursuit of numerous individual lawsuits would not be economically feasible for individual Class members, and certification as a class action will preserve judicial resources by allowing the Class common issues to be adjudicated in a single forum, avoiding the need for duplicative hearings and discovery in individual actions that are based on an identical set of facts. In addition, without a class action, it is likely that many members of the Class will remain unaware of the claims they may possess.

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

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

90. **Predominance.** The issues in this action are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

91. This proposed class action does not present any unique management difficulties.

FIRST CAUSE OF ACTION

BREACH OF IMPLIED CONTRACT

92. Plaintiff realleges and incorporates by reference all paragraphs above as if fully set forth herein.

93. In connection with their employment from Defendant, Plaintiff and Class members entrusted Defendant with their PII.

94. Defendant had an implied contract with Plaintiff and Class members that it would protect the PII it collected from them.

95. Plaintiff and Class members were required to deliver their PII to Defendant as part of the process of receiving employment. In doing so, they were of the belief that this information would be safely guarded.

96. Defendant accepted possession of Plaintiff's and Class members' PII for the purpose of providing services to them.

97. Through Defendant's individual provision of services, it knew or should have known that it must protect Plaintiff's and Class members' confidential PII in accordance with Defendant's stated policies and industry best practices.

98. Pursuant to these implied contracts, Defendant agreed to certain implied promises to Plaintiff and Class members, including but not limited to the following: (i) taking steps to ensure that anyone who is granted access to PII also protects the confidentiality of that data; (ii) taking steps to ensure that the PII placed in control of Defendant's employees is restricted and limited only to achieve authorized business purposes; (iii) restricting PII access only to employees and/or agents who are qualified and trained; (iv) designing and implementing appropriate retention policies to protect Private Information; (v) applying or requiring proper encryption and/or the

separation of different data sets containing PII; (vi) implementing multifactor authentication for access to PII; and (vii) taking other steps to protect against foreseeable breaches.

99. In entering into such implied contract, Plaintiff and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

100. Defendant violated these implied contracts and these implied promises by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class members' PII.

101. Plaintiff's and Class members' Private Information would not have been entrusted to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

102. Plaintiff and Class members fully and adequately performed their obligations under their implied contracts with Defendant.

103. Plaintiff and Class members have been damaged by Defendant's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein. Plaintiff and Class members seek damages, including restitution, actual damages, nominal damages, and any other awardable form of damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION

NEGLIGENCE/NEGLIGENCE PER SE

104. Plaintiff realleges and incorporates by reference all paragraphs above as if fully set forth herein.

105. Defendant required Plaintiff and the Class members to submit non-public personal information in order to obtain employment.

106. Plaintiff and the Class members are individuals who provided certain PII to Defendant including, and at a minimum, the PII described above.

107. Defendant had full knowledge of the sensitivity of the PII to which it was entrusted and the types of harm that Plaintiff and Class members could and would suffer if the information were wrongfully disclosed.

108. Defendant had a duty to Plaintiff each Class member to exercise reasonable care in holding, safeguarding and protecting that information.

109. Plaintiff and the Class members were the foreseeable victims of any inadequate safety and security practices.

110. The Class members had no ability to protect their data in Defendant's possession.

111. By collecting and storing this data in its computer property, and by sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property — and Plaintiff and the Class members' PII held within it — to prevent disclosure of the information and to safeguard the information from theft.

112. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

113. Defendant owed a duty of care to safeguard the PII of Plaintiff and Class members in its custody. This duty of care arises because Defendant knew of a foreseeable risk to the data security systems it used. Defendant knew of this foreseeable risk because of the explosion of data breach incidents involving consumer goods and services providers detailed above and in the news. Despite its knowledge of this foreseeable risk, Defendant failed to implement reasonable security measures.

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

115. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

116. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

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

118. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect the Class members’ PII.

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

- a. Failing to adopt, implement and maintain adequate security measures to safeguard Class members’ PII;
- b. Failing to adequately monitor the security of its networks and systems;
- c. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to Class members’ PII;

e. Failing to detect in a timely manner that Class members' PII had been compromised;

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

g. Failing to have mitigation and back-up plans in place in the event of a cyber- attack and data breach.

120. It was foreseeable that Defendant's failure to use reasonable measures to protect Class members' PII would result in injury to Plaintiff and Class members.

121. Further, the breach of security was reasonably foreseeable given the known high frequency of hacking incidents, cyberattacks, and data breaches in the consumer goods and services industry.

122. It was therefore foreseeable that the failure to adequately safeguard Class members' PII would result in one or more types of injuries to Class members.

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

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

REQUEST FOR RELIEF

WHEREFORE, Plaintiff Johnston, on his own behalf and on behalf of all others similarly situated, prays for relief as follows:

- A. For an Order certifying this case as a class action and appointing Plaintiff and his counsel to represent the Class;
- B. For an award of actual damages, compensatory damages, statutory damages, nominal damages and statutory penalties, in an amount to be determined, as allowable by law;
- C. For an award of damages, equitable, and injunctive relief, as well as reasonable attorneys' fees and costs, on behalf of themselves and the Class.
- D. For an award of punitive damages, as allowable by law;
- E. For injunctive and other equitable relief to ensure the protection of the sensitive information of Plaintiff and the Class which remains in Defendant's possession.
- F. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- G. Pre- and post-judgment interest on any amounts awarded; and
- H. Such other and further relief as the Court may deem just and proper.

I. JURY TRIAL DEMAND

125. Plaintiff hereby demands a trial by jury of all claims so triable.

DATED: October 24, 2026

Respectfully submitted,

/s/ Blake Hunter Yagman

Blake Hunter Yagman

YAGMAN PLLC

The Chrysler Building

405 Lexington Avenue, 26th Floor

New York, New York 10174

Tel.: 929-709-1493

Email: *blake.yagman@yagmanpllc.com*

*Attorneys for Plaintiff Johnston
and the Proposed Class*

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [NBCUniversal Data Breach: Class Action Lawsuit Filed Over Allegedly Inadequate Cybersecurity Measures](#)
