BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
Joshua B. Glatt (State Bar No. 354064)
1990 North California Blvd., 9th Floor
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com
jglatt@bursor.com

Attorneys for Plaintiff and the Putative Classes

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

MAX AGRESS, individually and on behalf of all others similarly situated,

Plaintiff,

v.

CRUNCHYROLL, LLC,

Defendant.

Case No.:

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Max Agress ("Plaintiff") brings this action individually and on behalf of all others similarly situated against Defendant Crunchyroll, LLC ("Crunchyroll" or "Defendant"). Plaintiff makes the following allegations pursuant to the investigation of his counsel and based upon information and belief, except as to allegations specifically pertaining to himself, which are based on personal knowledge.

NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit on behalf of all individuals who have subscribed to Defendant's on-demand streaming service.

2. Plaintiff seeks to hold Defendant responsible for the injuries Defendant inflicted on Plaintiff and thousands of similarly situated persons ("Class Members") due to Defendant's impermissibly inadequate data security, which caused the personally identifying information ("PII") such as the email address, credit card information, and IP address of Plaintiff and those similarly situated to be exfiltrated by unauthorized hackers (the "Data Breach" or "Breach") at a still undetermined and/or unconfirmed time. The Breach was made public on or around March 22, 2026.[1]

JURISDICTION AND VENUE

3. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is located in this District.

4. This Court has subject matter and diversity jurisdiction over this Action under 28 U.S.C. § 1332(d)(2)(A), as amended by the Class Action Fairness Act of 2005 ("CAFA"), because this is a class action wherein the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed Classes, and at least one Class Member is a citizen of a state different from Defendant.

[1] Gandharv Walia, *Who are ShinyHunters and What is Telus Digital? Crunchyroll Data Breach Explained. Here's How Much and What Kind of Sony Anime Streamer User Data was Stolen and What Should Users Do Now*, The Economic Times (Mar. 23, 2026), https://cybernews.com/security/crunchyroll-data-breach-telus-hack-users/.

5. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial portion of the events giving rise to Plaintiff's claims occurred in this District and because Defendant's principal place of business is located in this District.

THE PARTIES

6. Plaintiff Max Agress is a natural person and citizen of California who resides in Berkeley, California. Since 2013, Plaintiff Agress has been an annual subscriber to Defendant's on-demand streaming service. In creating his account, he provided Defendant with an e-mail address and his name. Plaintiff's membership is paid for through his PayPal account which contains his name and personally identifying information. On several occasions during his subscription, Plaintiff Agress has contacted Defendant's customer support.

7. Defendant Crunchyroll, LLC is a limited liability company organized under the laws of Delaware with a principal place of business in San Francisco, California. Defendant owns and operates its subscription streaming service that offers consumers who pay a monthly subscription price access to thousands of on-demand anime titles.

FACTUAL ALLEGATIONS

A. Background On Data Breaches

8. A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so.[2]

9. Data breaches are becoming increasingly more common and harmful. In 2014, 783 data breaches were reported, with at least 85.61 million total records exposed.[3] In 2019, 3,800 data breaches were reported, with at least 4.1 billion total records exposed.[4] The average cost of a data breach in the United States in 2019 was $8.19 million.[5]

10. Consumers are harmed in a variety of ways by data breaches. First, consumers are

[2] *See* Juliana de Groot, *The History of Data Breaches*, Fortra (Nov. 12, 2018), https://digitalguardian.com/blog/history-data-breaches.

[3] *See id*.

[4] *See* Dan Rafter, *2019 Data Breaches: 4 Billion Records Breached So Far*, Norton (Aug. 18, 2018), https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html.

[5] *See* IBM Security, *Cost of a Data Breach Report* (2019), https://insights.integrity360.com/hubfs/2019-cost-of-a-data-breach-report-04_03025203USEN.pdf.

harmed financially. According to the IBM and Ponemon Institute's 2019 "Cost of a Data Breach" report, the average cost of a data breach per consumer was $150 per record.[6] However, other estimates have placed the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity theft—a common result of data breaches—was $298 dollars.[7] And in 2019, Javelin Strategy & Research compiled consumer complaints from the U.S. Federal Trade Commission ("FTC") and indicated that the median out-of-pocket cost to consumers for identity theft was $375.[8]

11. Identity theft is one of the most problematic harms resulting from a data breach. With access to an individual's PII, criminals can do more than just empty a victim's bank account – they can also commit all manner of fraud, including obtaining a driver's license or official identification card in the victim's name, but with the thief's picture. In addition, identity thieves may obtain a job, rent a house, or receive medical services in the victim's name. Identity thieves 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.[9]

12. Consumers are also harmed by the time they spend rectifying the effects of a data breach. A Presidential identity theft report from 2007 states that:

> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts, open new ones, and

[6] *See id.*

[7] *See* Norton by Symantec, *2013 Norton Report* (2013), https://www.hearst.com/documents/33329/653025/2013+Norton+Report.pdf/9042fbe0-7640-de50-63b1-a0915ff91f4a?t=1581612867150.

[8] *See* Insurance Information Institute, *Facts + Statistics: Identity Theft and Cybercrime*, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (citing the Javelin report).

[9] *See* U.S. Federal Trade Commission, *Warning Signs of Identity Theft*, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft.

dispute charges with individual creditors.[10]

13. Further, the effects of a data breach on consumers are not temporary. In a report issued by the U.S. Government Accountability Office ("GAO"), the GAO found that "stolen data may be held for up to a year or more before being used to commit identity theft," and "fraudulent use of [stolen information] may continue for years" after the stolen information is posted on the Internet.[11] Thus, consumers can lose years' worth of time dealing with a data breach.

14. The existence of these problems is not always immediately ascertainable. As the GAO Report describes:

> [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 has been sold or posted on the web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

15. Consumers are also harmed by the lost value of their data. PII represents important, highly valuable property rights.[12] PII can be easily commodified, allowing the information to be bought and sold.[13] This information "has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[14]

16. Thus, when consumers' PII is disclosed without their consent, consumers are deprived of both the ability to choose what is done with their information as well as the full monetary value of their information.

---

[10] U.S. Federal Trade Commission, *The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan* (Apr. 2007), https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf.

[11] Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 694 (7th Cir. 2015) (citing U.S. Gov't Accountability Office, GAO–07–737, Report to Congressional Requesters: Personal Information (2007)).

[12] *See* John T. Soma et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J. L. & Tech. 11, at 3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

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

[14] *See* Soma, *supra*, note 12.

B. The Crunchyroll Data Breach

17. On March 22, 2026, International Cyber Digest released a tweet that Crunchyroll was the subject of a data breach through its outsourcing partner in India: "An employee of their outsourcing partner Telus had executed malware on his system, which gave a threat actor access to Crunchyroll's environment."[15] Telus is a business process outsourcing company that Defendant contracts with to process customer support inquiries from its consumers.

18. "Screenshots shared with reporters and researchers allegedly show full names, usernames, email addresses, IP addresses, approximate location data, and the text of user support exchanges. No full payment card data appears in the samples, though partial card details shared voluntarily in tickets (such as last four digits or expiration dates) may be in scope."[16] The extent of what hackers took from Defendant is still being investigated.

19. Despite the Breach not being made public until March 22, 2026, the news came after a threat actor contacted prominent, independent technology news publication BleepingComputer, stating that they committed the Breach on March 12, 2026, at 9:00 PM ET.[17]

20. By executing malware on the workstation of an employee within Telus, a business process outsourcing provider that supports Crunchyroll's customer operations, the hacker gained access to the corporate environment, including customer support and ticketing infrastructure.[18]

21. The hacker allegedly maintained access to the corporate environment for 24 hours, and, as a result of the Breach, downloaded eight (8) million support ticket records from

---

[15] International Cyber Digest (@intcyberdigest), X (Mar. 22, 2026, at 07:41 ET), https://x.com/IntCyberDigest/status/2035864555805413448?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E2035864555805413448%7Ctwgr%5E23203d6d30ee33831eff1ac9049c43a6920a01f6%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.pcmag.com%2Fnews%2Fcrunchyroll-investigating-possible-breach-involving-100gb-of-user-data.

[16] Gregory Zuckerman, *Hackers Claim Crunchyroll Breach Exposes 7 Million Users,* FINDARTICLES (Mar. 23, 2026) https://www.findarticles.com/hackers-claim-crunchyroll-breach-exposes-7-million-users/.

[17] *See* Lawrence Abrams, *Crunchyroll Probes Breach After Hacker Claims to Steal 6.8M Users' Data*, BleepingComputer (Mar. 23, 2026), https://www.bleepingcomputer.com/news/security/crunchyroll-probes-breach-after-hacker-claims-to-steal-68m-users-data/.

[18] Any Priya, *Crunchyroll Breach: Hackers Claim 100GB of User Data Stolen*, Cyber Press (Mar. 23, 2026), https://cyberpress.org/crunchyroll-breach-hackers-claim-100gb-of-user-data-stolen/.

Crunchyroll's Zendesk instance, allegedly containing 6.8 million unique email addresses.[19]

22. Business process outsourcing providers, like Telus, are oftentimes used by companies to reduce operating costs and improve efficiency. However, business process outsourcing providers are often targets for hackers because they handle and store large amounts of sensitive client information and may not have the same level of security as the companies they work for.[20]

23. Once sensitive data is exfiltrated from a network, it may be sold on the black market, used to execute further cyberattacks, or held hostage in exchange for exorbitant fees as part of a ransomware attack.[21]

24. Indeed, "[s]eparate researchers … reported reviewing screenshots and said the dataset could total about 100GB. SOCRadar noted a same-day posting on a criminal forum titled 'Crunchyroll email and IP,' accompanied by obscured samples that appear consistent with the claims."[22]

25. Despite the attack reportedly occurring on March 12, 2026, Crunchyroll did not release a statement that it was investigating the matter until March 23, 2026.[23]

C. Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' Valuable PII

26. Defendant collected, retained, and stored the PII of Plaintiff and Class Members and derived a substantial economic benefit from that PII. But for the collection of Plaintiff's and Class Members' PII, Defendant would not be able to perform its services.

27. Individuals, like Plaintiff and Class Members, who subscribe to Defendant's streaming service, were required to entrust Defendant with sensitive, non-public PII, to gain access

---

[19] *See* Abrams, *supra* note 17.

[20] Sentinel One, *What is BPO (Business Process Outsourcing)?*, https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-business-process-outsourcing-bpo/ (last updated July 3, 2025).

[21] IBM, *What is Data Exfiltration?*, https://www.ibm.com/think/topics/data-exfiltration (last visited Mar. 23, 2026).

[22] *See* Zuckerman, *supra* note 16.

[23] *See* Abrams, *supra* note 17.

to its on-demand titles. Defendant retains this information for many years, even after the consumer relationship has ended.

28. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible from protecting the PII from disclosure.

29. Additionally, Defendant made promises and representations to its consumers, including Plaintiff and Class Members, that the PII collected from them would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

30. Indeed, Defendant's Privacy Policy provides that it: "takes reasonable measures to protect Personal Information we collect from loss, theft, misuse and unauthorized access, disclosure, alteration, and destruction."[24]

31. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would keep their sensitive PII confidential, maintain its system security, use the PII for business purposes only, and to only disclose the information to authorized and trusted personnel.

32. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumers' PII safe and confidential.

33. The information held by Defendant in its computer systems at the time of the Breach reportedly includes individuals' email addresses, credit card details, and IP addresses.[25]

34. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen

[24] Sony Pictures, *Privacy Policy*, https://www.sonypictures.com/corp/privacy.html (last visited Mar. 23, 2026).

[25] *See* Abrams, *supra* note 16.

identity credentials.[26]

D. Defendant Failed to Comply with FTC Guidelines

33. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an 'unfair practice' in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

34. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Businesses, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer 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. 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 into 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.

35. 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 the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

36. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by treating the failure to employ reasonable and appropriate

[26] Anita George, *Your Personal Data is For Sale on the Dark Web. Here's How Much it Costs*, Digital Trends, https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (Oct. 16, 2019).

measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

37. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

38. Defendant was at all times fully aware of its obligation to protect the PII of its consumers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

E. Defendant Failed to Comply with Industry Standards

39. Despite its alleged commitment to taking reasonable measures to secure sensitive PII, Defendant does not follow industry standard practices in securing PII.

40. Some industry best practices that should be implemented by entertainment companies dealing with sensitive PII, like Defendant, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi- factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

41. Other best cybersecurity practices that are standard in the entertainment industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

42. 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.

43. Defendant failed to comply with these accepted standards in the entertainment industry, thereby permitting the Data Breach to occur.

F. Common Injuries and Experiences of Plaintiff and Class Members

44. Plaintiff and Class Members are individuals who have subscribed to Defendant's on-demand anime streaming service. In doing so, Plaintiff and Class Members were required to provide their PII to Defendant, including but not limited to, their email address and credit card information.

45. At the time of the data breach, Defendant retained Plaintiff's, as an active subscriber, PII in its system.

46. Plaintiff is very careful about sharing his sensitive PII. Plaintiff regularly monitors his credit and banking information and have increased this monitoring since learning of the Breach.

47. Plaintiff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

48. When Defendant released a statement relating to the Data Breach, it deliberately underplayed the Breach's severity and obfuscated the nature of the Breach. To date, Defendant has failed to explain how the Breach occurred (what security weakness was exploited), what exact data elements of each affected individual were compromised, who the Breach was perpetrated by, and the extent to which those data elements were compromised.

49. Because of the Data Breach, Defendant inflicted injuries upon Plaintiff and Class Members, including but not limited to, their PII ending up in the possession of criminals, the risk of identity theft, invasion of privacy, the continued mitigation of the materialized risk of identity theft, and the loss of benefit of the bargain.

50. Plaintiff and Class Members entrusted their PII to Defendant and were deprived of the benefit of their bargain. Plaintiff had the reasonable expectation and understanding that Defendant would take—at minimum—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify them of any data security incidents. After all, Plaintiff would not have entrusted his PII to any entity that used Defendant's services had he known that Defendant would not take reasonable steps to safeguard his information. Accordingly, Plaintiff and Class Members received a service that was of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

51. The unencrypted PII of Plaintiff and Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

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

53. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes.

54. Plaintiff and Class Members suffered actual injury from having their PII compromised in the Data Breach including, but not limited to, (a) damage to and diminution in the value of their PII—a form of property that Defendant obtained from Plaintiff; (b) violation of their privacy rights; (c) the likely theft of their PII; (d) fraudulent activity resulting from the Breach; and (e) present and continuing injury arising from the increased risk of additional identity theft and fraud.

55. As a result of the Data Breach, Plaintiff and Class Members also suffered emotional distress because of the release of their PII—which they believed would be protected from unauthorized access and disclosure. Now, Plaintiffs and Class Members will suffer anxiety about unauthorized parties viewing, selling, and/or using their PII for nefarious purposes like identity theft and fraud.

56. Plaintiff and Class Members have a continuing interest in ensuring that their PII, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

57. Defendant's use of business process outsourcing providers which are frequently targeted by hackers, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has failed to adequately protect the PII of Plaintiff and potentially thousands of members of the proposed Class to unscrupulous operators, con artists, and outright criminals.

58. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and the Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

CLASS ALLEGATIONS

59. ***Class Definition***: Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 on behalf of the following Class and Subclass of similarly situated individuals:

(a) ***Nationwide Class.*** Plaintiff seeks to represent a class of similarly situated individuals, defined as all persons in the United States whose PII was exposed in Defendant's March 2026 Data Breach (the "Class" or "Nationwide Class").

(b) ***California Subclass.*** Plaintiff also seeks to represent a subclass of all California residents whose PII was exposed in Defendant's March 2026 Data Breach (the "California Subclass").

60. Excluded from the Class are: (1) Defendant and its officers, directors, employees, principals, affiliated entities, controlling entities, and other affiliates; (2) the agents, affiliates, legal

representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

61. Plaintiff reserves the right to amend the definition of the Class and Subclass if discovery or further investigation reveals that the Class or Subclass should be expanded or otherwise modified.

62. ***Numerosity.*** Members of the Class and Subclass are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class and Subclass number in the millions. The precise number of Class Members and their identities are unknown to Plaintiff at this time but may be determined through discovery. Class Members may be notified of the pendency of this action by mail and/or publication through the distribution records of Defendant and third-party retailers and vendors.

63. ***Commonality and Predominance***. Common questions of law and fact exist as to all Class and Subclass Members and predominate over questions affecting only individual Class and Subclass Members. Common legal and factual questions include, but are not limited to: (a) whether Defendant knew or should have known that their systems were vulnerable to unauthorized access; (b) whether Defendant failed to take adequate and reasonable measures to ensure their data systems were protected; (c) whether Defendant failed to take available steps to prevent and stop the breach from happening; (d) whether Defendant owed a legal duty to Plaintiff and Class Members to protect their PII; (e) whether Defendant breached any duty to Plaintiff and Class Members by failing to exercise due care in protecting their PII; (f) whether Plaintiff and Class Members are entitled to actual, statutory, or other forms of damages, and/or other form of monetary relief; (g) whether Plaintiff and Class Members are entitled to equitable relief, including, but not limited to, injunctive relief or restitution; and (h) whether Plaintiff and Members of the Class and Subclass are entitled to attorneys' fees and costs.

64. ***Typicality.*** The claims of the named Plaintiff are typical of the claims of the Class and Subclass in that Plaintiff and members of the proposed Class and Subclass were subject to the data breach and had their PII accessed by and/or disclosed to unauthorized third parties.

65. ***Adequacy.*** Plaintiff is an adequate representative of the Class and Subclass because Plaintiff has no interests antagonistic to Class and Subclass Members' interests, Plaintiff has retained counsel with considerable experience and success in prosecuting complex class actions and consumer protection cases, and Plaintiff and the undersigned counsel intend to prosecute this action vigorously. The interests of the Class and Subclass Members will be fairly and adequately protected by Plaintiff and Plaintiff's counsel.

66. ***Declaratory and Injunctive Relief.*** The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members that would establish incompatible standards of conduct for Defendant. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class members and impair their interests. Defendant has acted and/or refused to act on grounds generally applicable to the Class, making injunctive relief or corresponding declaratory relief appropriate.

67. ***Superiority***. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Each individual Class and Subclass Member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In 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 on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of liability issues. Thus, the Class and Subclass are readily definable and prosecution as a class action avoids repetitious litigation and duplicative litigation costs, conserves judicial resources, ensures uniformity of decisions, and permits claims to be handled in an orderly and expeditious manner.

68. Defendant has acted or failed to act on grounds generally applicable to the Class and Subclass, thereby making appropriate final injunctive relief with respect to the Class and Subclass as a whole.

69. Without a class action, Defendant will continue a course of action that will result in further damages to Plaintiff and members of the Class and Subclass and will likely retain the benefits of their wrongdoing.

70. Based on the foregoing allegations, Plaintiff's claims for relief include those set forth below.

COUNT I
Negligence and Negligence *Per Se*
(On Behalf Of The Nationwide Class And California Subclass)

71. Plaintiff hereby re-alleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

72. Plaintiff brings this claim individually and on behalf of the members of the proposed Nationwide Class and California Subclass against Defendant.

73. Defendant gathered and stored the PII of Plaintiff and Class Members as part of its business of soliciting its services to its consumers, which solicitations and services affect commerce.

74. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would safeguard their information.

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

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

77. Defendant had a duty to employ reasonable security measures under Section 5 of the FTCA, 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.

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

79. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of being consumers of Defendant.

80. 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.

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

82. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former consumers' PII it was no longer required to retain pursuant to regulations.

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

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

85. Defendant breached its duties, pursuant to the FTCA and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

(a) Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

(b) Failing to adequately monitor the security of their networks and systems;

(c) Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;

(d) Allowing unauthorized access to Class Members' PII;

(e) Failing to remove former consumers' PII it was no longer required to retain pursuant to regulations; and

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

86. Defendant violated Section 5 of the FTCA by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein.

87. Plaintiff and Class Members were within the class of persons the FTCA was intended to protect and the type of harm that resulted from the Data Breach was the type of harm it was intended to guard against.

88. Defendant's violation of Section 5 of the FTCA constitutes negligence *per se*.

89. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

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

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

92. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

93. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in

collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

94. 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.

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

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

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

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

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

100. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed

up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

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

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

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

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

105. 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) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach of Implied Contract
(On Behalf Of The Nationwide Class And California Subclass)

106. Plaintiff hereby re-alleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

107. Plaintiff brings this claim individually and on behalf of the members of the proposed Nationwide Class and California Subclass against Defendant.

108. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of receiving services from Defendant.

109. Plaintiff and the Class entrusted their PII to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and

protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

110. In entering into such implied contracts, 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.

111. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

112. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

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

114. In accepting the PII of Plaintiff and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the PII from unauthorized access or disclosure.

115. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

116. On information and belief, Defendant further promised to take reasonable measures to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

117. Plaintiff and Class Members paid money and provided their PII to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

118. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

119. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

120. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

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

122. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

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

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

COUNT III
Unjust Enrichment / Restitution
(On Behalf of the Nationwide Class And California Subclass)

125. Plaintiff hereby re-alleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

126. This count is pleaded in the alternative to the Breach of Implied Contract claim above (Count II).

127. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they paid for a subscription service with Defendant and in so doing also provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the services that were the subject of the transaction and should have had their PII protected with adequate data security.

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

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

130. Defendant acquired the PII through inequitable record retention as it failed to disclose the inadequate data security practices previously alleged.

131. If Plaintiff and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would not have entrusted their PII at Defendant or obtained subscription services from Defendant.

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

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

134. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed

up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

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

136. Plaintiff has no adequate remedy at law for this claim. Plaintiff plead his claim for unjust enrichment in the alternative, which inherently would necessitate a finding of no adequate remedy at law. Alternatively, legal remedies available to Plaintiff are inadequate because they are not "equally prompt and certain and in other ways efficient" as equitable relief. *American Life Ins. Co. v. Stewart*, 300 U.S. 203, 214 (1937); *see also U.S. v. Bluitt*, 815 F. Supp. 1314, 1317 (N.D. Cal. 1992) ("the 'mere existence' of a possible legal remedy is not sufficient to warrant denial of equitable relief"); *Quist v. Empire Water Co.*, 2014 Cal. 646, 643 (1928) ("The mere fact that there may be a remedy at law does not oust the jurisdiction of a court of equity. To have this effect, the remedy must also be speedy, adequate, and efficacious to the end in view … It must reach the whole mischief and secure the whole right of the party in a perfect manner at the present time and not in the future"). Furthermore:

(a) To the extent damages are available here, damages are not equally certain as restitution because the standard that governs ordering restitution is different than the standard that governs damages. Hence, the Court may award restitution even if it determines that Plaintiff fails to sufficiently adduce evidence to support an award of damages.

(b) Damages and restitution are not necessarily the same amount. Unlike damages, restitution is not limited to the amount of money defendant wrongfully acquired plus the legal rate of interest. Equitable relief, including restitution, entitles Plaintiff to recover all profits from the wrongdoing, even

where the original funds taken have grown far greater than the legal rate of interest would recognize. Plaintiff seeks such relief here.

(c) Legal claims for damages are not equally certain as restitution because claims under the UCL and unjust enrichment entail few elements.

137. A claimant otherwise entitled to a remedy for unjust enrichment, including a remedy originating in equity, need not demonstrate the inadequacy of available remedies at law." Restatement (Third) of Restitution, § 4(2).

COUNT IV
Violation of Cal. Civ. Code § 1798.81.5
(On Behalf Of The California Subclass)

138. Plaintiff hereby re-alleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

139. Cal. Civ. Code § 1798.81.5 states that it is "the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

140. Plaintiff is a California citizen who provided personal information to Defendant, as that term is defined.

141. Plaintiff's personal information includes his first initial and last name, credit card number, a user name, and e-mail address associated with his account. *See* Cal. Civ. Code § (1)(A)(iii).

142. Defendant contracted with a third party, Telus, which had access to—and did negligently provide access to—Plaintiff's personal information to hackers.

143. The statute mandates that "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

144. Defendant "owns" and "licenses" Plaintiff's personal information, as defined, because Defendant retains Plaintiff's and Class Members' personal information as part of its internal customer account and for the purpose of using that information in transactions with the person.

145. Cal. Civ. Code § 1798.81.5(c) requires that "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party … shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

146. Defendant failed to take reasonable care to meet its obligations under the statute and failed to ensure that its third-party contractor had procedures and safeguards in place to ensure that Plaintiff's personal information was properly protected.

147. Plaintiff and Class Members seek an order declaring that Defendant violated Cal. Civ. Code § 1798.81.5 and an order requiring that Defendant comply with the statute pursuant to Cal. Civ. Code § 1798.84(e).

COUNT V
Violations of California's Unfair Competition Law ("UCL"),
California Business & Professions Code §§ 17200, *et seq*.
(On Behalf Of The California Subclass)

148. Plaintiff hereby re-alleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

149. Plaintiff brings this claim individually and on behalf of the members of the proposed California Subclass against Defendants.

150. Crunchyroll is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

151. Crunchyroll violated Cal. Bus. & Prof. Code § 17200, *et seq*. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

152. Crunchyroll's unlawful, unfair, and deceptive acts and practices include:

(a) Crunchyroll failed to implement and maintain reasonable security measures to protect Plaintiff's and Class Members' PII from unauthorized disclosure,

release, data breaches, and theft, which was a direct and proximate cause of the Data Breach.

(b) Crunchyroll's failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTCA 15 U.S.C. § 45, California's Consumer Records Act, Cal. Civ. Code § 1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.

(c) Crunchyroll's failure to implement and maintain reasonable security measures also resulted in substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Crunchyroll's grossly inadequate security, consumers could not have reasonably avoided the harms that Crunchyroll caused.

(d) Crunchyroll engaged in unlawful business practices by violating Cal. Civ. Code § 1798.81.5 and Cal. Civ. Code § 1750, *et seq*.

(e) Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45;

153. Crunchyroll's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Crunchyroll's data security and ability to protect the confidentiality of consumers' PII.

154. As a direct and proximate result of Crunchyroll's unfair, unlawful, and fraudulent acts and practices, Plaintiff and Class Members were injured and suffered monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Crunchyroll's services; loss of

the value of access to their PII; and the value of identity protection services made necessary by the Breach.

155. Crunchyroll acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and Class Members' rights.

156. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Crunchyroll's unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT VI
Declaratory Judgment
(On Behalf of the Nationwide Class And California Subclass)

157. Plaintiff hereby re-alleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

158. Plaintiff brings this claim individually and on behalf of the members of the proposed Nationwide Class and California Subclass against Defendant.

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

160. An actual controversy has arisen in the wake of the Crunchyroll Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' PII and whether Crunchyroll is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff alleges that Crunchyroll's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of their PII and remains at imminent risk that further compromises of their PII will occur in the future.

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

a. Crunchyroll continues to owe a legal duty to secure consumers' PII and to

timely notify consumers of a data breach under the common law, Section 5 of the FTCA, and various state statutes; and

b. Crunchyroll continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII.

162. The Court also should issue corresponding prospective injunctive relief requiring Crunchyroll to employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

163. If an injunction is not issued, Plaintiff will suffer irreparable injury, and he lacks an adequate legal remedy in the event of another data breach at Crunchyroll. The risk of another such breach is real, immediate, and substantial. If another breach at Crunchyroll occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

164. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Crunchyroll if an injunction is issued. Among other things, if another massive data breach occurs at Crunchyroll, Plaintiff will likely be subjected to identify theft and other damage. On the other hand, the cost to Crunchyroll of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Crunchyroll has a pre-existing legal obligation to employ such measures.

165. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Crunchyroll, thus eliminating the additional injuries that would result to Plaintiff and the millions of consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendants, as follows:

(a) For a determination that this is a proper class action;

(b) For an order certifying the proposed Nationwide Class and the California Subclass under Rule 23 of the Federal Rules of Civil Procedure, naming Plaintiff as representative of the proposed Class and Subclass, and naming Plaintiff's attorneys as Class Counsel to represent the Class and Subclass;

(c) For an order declaring Defendant's conduct violates the statutes referenced herein;

(d) For an order finding in favor of Plaintiff and members of the Class and Subclass on all counts asserted herein;

(e) For actual, compensatory, statutory, and/or punitive damages in amounts to be determined by the Court and/or jury;

(f) For prejudgment interest on all amounts awarded;

(g) For an order of restitution and all other forms of equitable monetary relief;

(h) For injunctive relief as pleaded or as the Court may deem proper;

(i) For an order awarding Plaintiff and members of the Class and Subclass their reasonable attorneys' fees and reimbursement of litigation expenses and costs of suit; and

(j) For such other and further relief as the Court may deem proper.

JURY DEMAND

Plaintiff demands a trial by jury on all causes of action and issues so triable.

Dated: March 24, 2026

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ L. Timothy Fisher*

L. Timothy Fisher (State Bar No. 191626)
Joshua B. Glatt (State Bar No. 354064)
1990 North California Blvd., 9th Floor
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com
jglatt@bursor.com

Attorneys for Plaintiff and the Putative Classes

ClassAction.org
