

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

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

6 **NATURE OF THE ACTION**

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

9 2. Plaintiff seeks to hold Defendant responsible for the injuries Defendant inflicted on
10 Plaintiff and thousands of similarly situated persons (“Class Members”) due to Defendant’s
11 impermissibly inadequate data security, which caused the personally identifying information
12 (“PII”) such as the email address, credit card information, and IP address of Plaintiff and those
13 similarly situated to be exfiltrated by unauthorized hackers (the “Data Breach” or “Breach”) at a
14 still undetermined and/or unconfirmed time. The Breach was made public on or around March 22,
15 2026.¹

16 **JURISDICTION AND VENUE**

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

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

24
25
26 _____
27 ¹ Gandharv Walia, *Who are ShinyHunters and What is Telus Digital? Crunchyroll Data Breach*
28 *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/>.

1 harmed financially. According to the IBM and Ponemon Institute’s 2019 “Cost of a Data Breach”
2 report, the average cost of a data breach per consumer was \$150 per record.⁶ However, other
3 estimates have placed the costs even higher. The 2013 Norton Report estimated that the average
4 cost per victim of identity theft—a common result of data breaches—was \$298 dollars.⁷ And in
5 2019, Javelin Strategy & Research compiled consumer complaints from the U.S. Federal Trade
6 Commission (“FTC”) and indicated that the median out-of-pocket cost to consumers for identity
7 theft was \$375.⁸

8 11. Identity theft is one of the most problematic harms resulting from a data breach.
9 With access to an individual’s PII, criminals can do more than just empty a victim’s bank account
10 – they can also commit all manner of fraud, including obtaining a driver’s license or official
11 identification card in the victim’s name, but with the thief’s picture. In addition, identity thieves
12 may obtain a job, rent a house, or receive medical services in the victim’s name. Identity thieves
13 may even give the victim’s personal information to police during an arrest, resulting in an arrest
14 warrant being issued in the victim’s name.⁹

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

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

23 ⁶ See *id.*

24 ⁷ See Norton by Symantec, *2013 Norton Report* (2013),
<https://www.hearst.com/documents/33329/653025/2013+Norton+Report.pdf/9042fbc0-7640-de50-63b1-a0915ff91f4a?t=1581612867150>.

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

27 ⁹ See U.S. Federal Trade Commission, *Warning Signs of Identity Theft*,
28 <https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft>.

1 dispute charges with individual creditors.¹⁰

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

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

9 [L]aw enforcement officials told us that in some cases, stolen data may
10 be held for up to a year or more before being used to commit identity
11 theft. Further, once stolen, data has been sold or posted on the web,
12 fraudulent use of that information may continue for years. As a result,
13 studies that attempt to measure the harm resulting from data breaches
14 cannot necessarily rule out all future harm.

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

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

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

25 ¹¹ *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 694 (7th Cir. 2015) (citing U.S. Gov’t
26 Accountability Office, GAO–07–737, Report to Congressional Requesters: Personal Information
27 (2007)).

28 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.

1 **B. The Crunchyroll Data Breach**

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

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

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

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

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

20 _____
21 ¹⁵ International Cyber Digest (@intcyberdigest), X (Mar. 22, 2026, at 07:41 ET),
22 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.

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

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

28 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/>.

1 Crunchyroll’s Zendesk instance, allegedly containing 6.8 million unique email addresses.¹⁹

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

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

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

14 25. Despite the attack reportedly occurring on March 12, 2026, Crunchyroll did not
15 release a statement that it was investigating the matter until March 23, 2026.²³

16 **C. Defendant Acquires, Collects, and Stores Plaintiff’s and Class**
17 **Members’ Valuable PII**

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

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

23 ¹⁹ See Abrams, *supra* note 17.

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

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

28 ²² See Zuckerman, *supra* note 16.

²³ See Abrams, *supra* note 17.

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

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

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

10 30. Indeed, Defendant’s Privacy Policy provides that it: “takes reasonable measures to
11 protect Personal Information we collect from loss, theft, misuse and unauthorized access,
12 disclosure, alteration, and destruction.”²⁴

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

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

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

23 34. The PII of individuals remains of high value to criminals, as evidenced by the
24 prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen
25

26 _____
27 ²⁴ Sony Pictures, *Privacy Policy*, <https://www.sonypictures.com/corp/privacy.html> (last visited
28 Mar. 23, 2026).

²⁵ See Abrams, *supra* note 16.

1 identity credentials.²⁶

2 **D. Defendant Failed to Comply with FTC Guidelines**

3 33. The FTC has promulgated numerous guides for businesses which highlight the
4 importance of implementing reasonable data security practices. According to the FTC, the need for
5 data security should be factored into all business decision making. Indeed, the FTC has concluded
6 that a company's failure to maintain reasonable and appropriate data security for consumers'
7 sensitive personal information is an 'unfair practice' in violation of Section 5 of the Federal Trade
8 Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d
9 236 (3d Cir. 2015).

10 34. In October 2016, the FTC updated its publication, *Protecting Personal Information:*
11 *A Guide for Businesses*, which established cybersecurity guidelines for businesses. The guidelines
12 note that businesses should protect the personal consumer information that they keep, properly
13 dispose of personal information that is no longer needed, encrypt information stored on computer
14 networks, understand their network's vulnerabilities, and implement policies to correct any security
15 problems. The guidelines also recommend that businesses use an intrusion detection system to
16 expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is
17 attempting to hack into the system, watch for large amounts of data being transmitted from the
18 system, and have a response plan ready in the event of a breach.

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

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

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

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

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

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

12 **E. Defendant Failed to Comply with Industry Standards**

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

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

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

27 42. Defendant failed to meet the minimum standards of any of the following frameworks:
28 the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC- 1, PR.AC-3,

1 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,
2 DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security’s
3 Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity
4 readiness.

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

7 **F. Common Injuries and Experiences of Plaintiff and Class**
8 **Members**

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

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

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

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

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

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

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

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

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

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

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

28

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

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

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

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

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

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

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

14 67. **Superiority.** A class action is superior to all other available methods for the fair and
15 efficient adjudication of this controversy. Each individual Class and Subclass Member may lack the
16 resources to undergo the burden and expense of individual prosecution of the complex and extensive
17 litigation necessary to establish Defendant's liability. Individualized litigation increases the delay
18 and expense to all parties and multiplies the burden on the judicial system presented by the complex
19 legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent
20 or contradictory judgments. In contrast, the class action device presents far fewer management
21 difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive
22 supervision by a single court on the issue of Defendant's liability. Class treatment of the liability
23 issues will ensure that all claims and claimants are before this Court for consistent adjudication of
24 liability issues. Thus, the Class and Subclass are readily definable and prosecution as a class action
25 avoids repetitious litigation and duplicative litigation costs, conserves judicial resources, ensures
26 uniformity of decisions, and permits claims to be handled in an orderly and expeditious manner.

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

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

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

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

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

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

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

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

- 26 (a) Failing to adopt, implement, and maintain adequate security measures to
27 safeguard Class Members' PII;
- 28 (b) Failing to adequately monitor the security of their networks and systems;

- 1 (c) Failing to audit, monitor, or ensure the integrity of its vendor’s data security
- 2 practices;
- 3 (d) Allowing unauthorized access to Class Members’ PII;
- 4 (e) Failing to remove former consumers’ PII it was no longer required to retain
- 5 pursuant to regulations; and
- 6 (f) Failing to timely and adequately notify Class Members about the Data
- 7 Breach’s occurrence and scope, so that they could take appropriate steps to
- 8 mitigate the potential for identity theft and other damages.

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

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

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

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

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

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

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

26 93. Plaintiff and the Class were the foreseeable and probable victims of any inadequate
27 security practices and procedures. Defendant knew or should have known of the inherent risks in
28

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

3 94. It was therefore foreseeable that the failure to adequately safeguard Class Members'
4 PII would result in one or more types of injuries to Class Members.

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

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

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

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

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

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

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

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

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

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

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

14 105. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant
15 to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual
16 audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit
17 monitoring to all Class Members.

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

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

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

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

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

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

3 110. In entering into such implied contracts, Plaintiff and Class Members reasonably
4 believed and expected that Defendant's data security practices complied with relevant laws and
5 regulations and were consistent with industry standards.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

22 **COUNT III**

23 **Unjust Enrichment / Restitution**
24 **(On Behalf of the Nationwide Class And California Subclass)**

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

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

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

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

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

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

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

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

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

21 134. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members
22 have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of
23 PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with
24 attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain;
25 (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data
26 Breach; and (vii) the continued and certainly increased risk to their PII, which: (a) remains
27 unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed
28

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

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

8 136. Plaintiff has no adequate remedy at law for this claim. Plaintiff plead his claim for
9 unjust enrichment in the alternative, which inherently would necessitate a finding of no adequate
10 remedy at law. Alternatively, legal remedies available to Plaintiff are inadequate because they are
11 not "equally prompt and certain and in other ways efficient" as equitable relief. *American Life Ins.*
12 *Co. v. Stewart*, 300 U.S. 203, 214 (1937); *see also U.S. v. Bluit*, 815 F. Supp. 1314, 1317 (N.D. Cal.
13 1992) ("the 'mere existence' of a possible legal remedy is not sufficient to warrant denial of equitable
14 relief"); *Quist v. Empire Water Co.*, 2014 Cal. 646, 643 (1928) ("The mere fact that there may be a
15 remedy at law does not oust the jurisdiction of a court of equity. To have this effect, the remedy must
16 also be speedy, adequate, and efficacious to the end in view ... It must reach the whole mischief and
17 secure the whole right of the party in a perfect manner at the present time and not in the future").

18 Furthermore:

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

24 (b) Damages and restitution are not necessarily the same amount. Unlike
25 damages, restitution is not limited to the amount of money defendant
26 wrongfully acquired plus the legal rate of interest. Equitable relief, including
27 restitution, entitles Plaintiff to recover all profits from the wrongdoing, even
28

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

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

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

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

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

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

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

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

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

24 143. The statute mandates that “[a] business that owns, licenses, or maintains personal
25 information about a California resident shall implement and maintain reasonable security procedures
26 and practices appropriate to the nature of the information, to protect the personal information from
27 unauthorized access, destruction, use, modification, or disclosure.”
28

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

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

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

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

15 **COUNT V**
16 **Violations of California’s Unfair Competition Law (“UCL”),**
17 **California Business & Professions Code §§ 17200, *et seq.***
(On Behalf Of The California Subclass)

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

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

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

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

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

- 26 (a) Crunchyroll failed to implement and maintain reasonable security measures
27 to protect Plaintiff’s and Class Members’ PII from unauthorized disclosure,
28

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

3 (b) Crunchyroll’s failure to implement and maintain reasonable security measures
4 also was contrary to legislatively declared public policy that seeks to protect
5 consumers’ data and ensure that entities that are trusted with it use appropriate
6 security measures. These policies are reflected in laws, including the FTCA
7 15 U.S.C. § 45, California’s Consumer Records Act, Cal. Civ. Code §
8 1798.81.5, and California’s Consumer Privacy Act, Cal. Civ. Code §
9 1798.100.

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

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

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

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

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

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

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

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

9 **COUNT VI**
10 **Declaratory Judgment**
11 **(On Behalf of the Nationwide Class And California Subclass)**

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

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

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

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

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

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

- (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

This complaint is part of ClassAction.org's searchable [class action lawsuit database](#)
