

Jennie Lee Anderson (SBN 203586)

jennie@andrusanderson.com

ANDRUS ANDERSON LLP

155 Montgomery Street, Suite 900

San Francisco, CA 94104

Telephone: (415) 986-1400

Facsimile: (415) 986-1474

Elizabeth A. Fegan (*to be admitted pro hac vice*)

beth@feganscott.com

FEGAN SCOTT LLC

150 S. Wacker Dr., 24th Floor

Chicago, IL 60606

Telephone: (312) 741-1019

Facsimile: (312) 264-0100

Attorneys for Plaintiff (Additional Counsel Listed on Signature Page)

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CHRISTOPHER ROSIAK, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

ZYNGA INC.,

Defendant.

Case No. 20-cv-5674

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Table of Contents

1 I. INTRODUCTION 1

2 II. PARTIES 2

3 III. JURISDICTION AND VENUE 2

4 IV. INTRADISTRICT ASSIGNMENT..... 3

5 V. FACTS..... 3

6 A. Zynga provides “free” games in exchange for its users’ PII..... 3

7 B. Zynga collected PII from minors. 4

8 C. With only non-existent or outdated encryption systems in place to protect customer PII, the
9 PII of Plaintiff and the Class were stolen from Zynga..... 6

10 D. Zynga has failed to adequately notify and protect its customers since learning of the data
11 breach..... 8

12 E. Data breaches, like Zynga’s, cause financial, emotional, and physical harm to the victims,
13 including to Plaintiff and the Class..... 11

14 VI. CLASS ACTION ALLEGATIONS 13

15 VII. CLAIMS 15

16 **COUNT I - NEGLIGENCE** (on Behalf of Plaintiff and the Nationwide Class) 15

17 **COUNT II - NEGLIGENCE PER SE** (on Behalf of Plaintiff and the Nationwide Class)..... 18

18 **COUNT III - BREACH OF CONTRACT** (on Behalf of Plaintiff and the Nationwide Class) 19

19 **COUNT IV - BREACH OF IMPLIED CONTRACT** (on Behalf of Plaintiff and the
20 Nationwide Class)..... 20

21 **COUNT V - UNJUST ENRICHMENT** (on Behalf of Plaintiff and the Nationwide Class)..... 21

22 **COUNT VI - BREACH OF CONFIDENCE** (on Behalf of Plaintiff and the Nationwide Class)
23 23

24 **COUNT VII - VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW CAL.
25 BUS. & PROF. CODE, §§ 17200, ET SEQ.** (on Behalf of Plaintiff and the Nationwide Class)
26 24

27 **COUNT VIII - VIOLATIONS OF THE CALIFORNIA FALSE ADVERTISING LAW
28 CAL. BUS. & PROF. CODE § 17500, ET SEQ.** (on Behalf of Plaintiff and the Nationwide
Class)..... 27

**COUNT IX - VIOLATIONS OF THE CALIFORNIA CONSUMERS LEGAL REMEDIES
ACT, CAL. CIV. CODE § 1750, ET SEQ.** (on Behalf of Plaintiff and the Nationwide Class) 30

**COUNT X - ALTERNATIVE COUNT FOR VIOLATIONS OF STATE CONSUMER
PROTECTION ACTS** (on Behalf of Plaintiff and the Nationwide Class) 33

JURY DEMAND 37

1 Plaintiff Christopher Rosiak, individually and on behalf of all other persons similarly situated,
2 by and through their attorneys, for their Complaint against Defendant Zynga Inc., allege as follows:

3 **I. INTRODUCTION**

4 1. Defendant Zynga Inc. (“Zynga”) proclaims it is “a leading developer of the world’s
5 most popular social games that are played by millions of people around the world each day.” Zynga
6 promises that it has in place “reasonable and appropriate security measures to help protect the security
7 of your information both online and offline and to ensure that your data is treated securely....”

8 2. In fact, hundreds of millions of people, including Plaintiff, trusted and believed Zynga’s
9 promise to protect their personally-identifying information, including name, email address, Zynga ID
10 and password, Facebook ID and password and, in some instances, financial information given to
11 Zynga for purchases for games and other in-game items (collectively, “PII”).¹

12 3. Yet despite its promise, Zynga failed to protect its customers’ PII by, among other
13 things, using password encryption methods that were banned for use by federal governmental
14 agencies as early as 2010.

15 4. In September of 2019, Zynga’s customer data base was breached by a serial hacker who
16 had previously stolen and sold PII on the dark web. By current estimates, over 170 million Zynga
17 accounts were accessed (the “Zynga Data Breach”). Although Zynga had notice of the breach and
18 identified which of its customer accounts were accessed, Zynga never directly notified those
19 customers.

20 5. Since the Zynga Data Breach, Zynga’s customers have been exposed to credit and
21 identity theft, “credit stuffing,” phishing scams, and any other fraudulent conduct that a criminal mind
22 can concoct. Plaintiff has and will incur costs to mitigate the risk for the data breach, such as paying
23 for credit monitoring services, and will have to spend countless hours monitoring their credit reports
24 and credit card statements. Regardless of whether they have yet to incur out-of-pocket losses,

25 _____
26 ¹ As used throughout this Complaint, “PII” is defined as all information exposed by the Zynga
27 Data Breach that occurred on or around September 2019, including but not limited to all or any part or
28 combination of name, address, telephone number, email address, gender, Zynga login and password,
Facebook login and password, credit card information, and other personally identifying information.

1 Plaintiff and all Zynga customers whose PII was stolen remain subject to a pervasive, substantial, and
2 imminent risk of identity theft and fraud now and for years to come.

3 6. This class action is brought on behalf of all persons residing in the United States whose
4 PII was compromised in the Zynga Data Breach to redress the damages they have suffered and to
5 obtain appropriate equitable relief to mitigate the risk that Zynga will be breached in the future.

6 II. PARTIES

7 7. Plaintiff Christopher Rosiak is a resident and citizen of the State of Indiana and at all
8 relevant times resided in Dyer, Indiana. In or around December 18, 2011, Mr. Rosiak provided his PII
9 to Zynga in order to create an account to access and play the Zynga game *Hanging with Friends*. He
10 only played that Zynga game for a short period of time and no later than 2012, and deleted the
11 application from his phone sometime thereafter. He never agreed to Zynga's Terms of Service, or to
12 any Zynga arbitration provision, or to any Zynga class action waiver provision.

13 8. Mr. Rosiak's PII was stolen in the Zynga Data Breach. Mr. Rosiak did not receive any
14 notice from Zynga regarding the Zynga Data Breach, and only learned about it in December 2019 or
15 January 2020. Mr. Rosiak learned through IDnotify, an identity theft monitoring service, that his
16 email was accessed in the Zynga Data Breach.

17 9. Plaintiff Christopher Rosiak provided his PII to Zynga with the expectation and
18 understanding that Zynga would adequately protect and store the data. He believed that when he
19 deleted the application from his phone, that Zynga would not save or store his PII. If he had known
20 that Zynga would keep his PII and that its data security measures and protections were insufficient to
21 protect his PII, he would not have created a Zynga user account and downloaded and played Zynga
22 games. As a result, Plaintiff has been damaged.

23 10. Defendant Zynga Inc. is a Delaware corporation with its headquarters and principle
24 place of business in San Francisco, California.

25 III. JURISDICTION AND VENUE

26 11. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of
27 2005, 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of \$5,000,000 exclusive of
28

1 interest and costs, there are more than 100 putative Class members, and Zynga is a citizen of a state
2 different from that of at least one Class member.

3 12. This Court has personal jurisdiction over Zynga because Zynga is headquartered in this
4 state and regularly transacts business in this state.

5 13. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part
6 of the events or omissions giving rise to Plaintiff's claims occurred in this district, including decisions
7 made by Zynga related to and led to the Zynga Data Breach alleged herein.

8 IV. INTRADISTRICT ASSIGNMENT

9 14. Assignment to the San Francisco division of this district is appropriate under Civil Local
10 Rule 3-2 because a substantial part of the events or omissions which give rise to the claims occurred
11 in the San Francisco division.

12 V. FACTS

13 A. Zynga provides "free" games in exchange for its users' PII.

14 15. Zynga touts itself as "a leading developer of the world's most popular social games that
15 are played by millions of people around the world each day."² Zynga develops, markets, and operates
16 social games as live services played on the Internet, social networking sites, and mobile platforms in
17 the United States and internationally. It offers its online social games under the *Slots*, *Words With*
18 *Friends*, *Zynga Poker*, and *FarmVille* franchises. Zynga also provides advertising services to
19 advertising agencies and brokers.³

20 16. At the end of 2019, Zynga had an average of an estimated 66 million users.⁴ Zynga's
21 *Words with Friends* was the most popular mobile game in the United States in March 2017, with 13
22 million unique users for the month. It held that position in 2016 as well.⁵

23 _____
24 ² <https://www.zynga.com/#> (last visited 7/27/20).

25 ³ <https://www.crunchbase.com/organization/zynga#section-overview> (last visited 7/27/20).

26 ⁴ "Average monthly active users (MAU) of Zynga games from 4th quarter 2012 to 1st quarter 2020,"
found at <https://www.statista.com/statistics/273569/monthly-active-users-of-zynga-games/> (last
visited 7/27/20).

27 ⁵ "Words With Friends trumps Pokemon GO as most popular US mobile game in March 2017 with 13
28 million users" (5/4/17) found at [https://www.pocketgamer.biz/news/65662/words-with-friends-13-
million-users-march-2017/](https://www.pocketgamer.biz/news/65662/words-with-friends-13-million-users-march-2017/) (last visited 7/27/20).

1 17. Zynga's games are accessible on mobile platforms, Facebook, and other social
2 networks, as well as Zynga.com. Zynga offers a mix of paid and "free" games, which are available
3 for download. Zynga's "free" games are supported by in-game advertisements, in-game purchases,
4 and its collection of users' PII.

5 18. Zynga's exchange of "free" games for its users' PII has been extremely successful. In
6 January 2020, Zynga's CEO claimed that Zynga is "on track to be one of the fastest-growing – if not
7 the fastest-growing – gaming company at scale." In 2019, its stock gained 56%, eclipsing the S&P's
8 29% increase.⁶

9 19. To play a Zynga game, the consumer must create a Zynga user account by providing
10 their first name, last name, email address, and gender, and must create a password for the account. At
11 all relevant times and based upon information and belief, Zynga did not collect information regarding
12 a user's age or date of birth, and thus, minors were able to and did create Zynga accounts.

13 20. Zynga's customers have the option to link their Zynga account to their Facebook
14 account instead of providing an email address, which requires providing Zynga with the customer's
15 Facebook username and password. Based on information and belief, if the consumer downloads the
16 game on a mobile device, the Facebook information is mandatory.

17 21. Zynga retains its users' names, email addresses, login IDs and passwords, password
18 reset tokens, phone numbers, and Facebook IDs and passwords in its databases. When financial
19 information, such as credit card details, is provided for game purchases or in-app purchases, Zynga
20 retains that information as well.

21 **B. Zynga collected PII from minors.**

22 22. One study estimates that 8% of all mobile gamers are ages 13-17,⁷ and based upon
23 information and belief, Zynga is aware that a substantial portion of its user base has been and
24

25 ⁶ "FarmVille Maker Zynga Is Booming Again" (1/3/2020), found at
26 [https://www.bloomberg.com/news/articles/2020-01-03/zynga-is-booming-again-after-wilderness-
years-at-farmville-maker](https://www.bloomberg.com/news/articles/2020-01-03/zynga-is-booming-again-after-wilderness-years-at-farmville-maker) (last visited 7/27/20).

27 ⁷ "The Mobile Gaming Industry: Statistics, Revenue, Demographics, More [Infographic]," (2/6/19),
28 found at <https://mediakix.com/blog/mobile-gaming-industry-statistics-market-revenue/> (last visited
7/27/20).

1 continues to be minors.

2 23. In fact, Zynga acknowledged in Securities and Exchange Commission filings that it is
3 subject to laws and regulations concerning the protection of minors, and that the “increased attention
4 being given to the collection of data from minors” has required it to devote significant operational
5 resources and incur significant expenses.⁸

6 24. Zynga’s *PetVille* was the subject of an investigative report which exposed that Facebook
7 targeted Zynga’s game-playing minors, and duped those children and their parents out of money, in
8 some cases hundreds or even thousands of dollars, and then refused to refund the amounts.⁹

9 25. Facebook encouraged game developers such as Zynga to let children spend money
10 without their parents’ permission, which Facebook called “friendly fraud,” in an effort to maximize
11 revenues.¹⁰ The children oftentimes did not know that they were spending money because while these
12 games are free to download, they are packed with opportunities to spend actual money to advance
13 further. These cash payments are designed to look like items within the game, making it difficult for
14 a child to recognize that they are spending money.¹¹

15 26. Children’s PII is particularly attractive to identity thieves. Children’s credit reports are
16 clean, and minors do not check their credit reports or review monthly bills, which means thieves may
17 not get caught for years or even decades. And a child’s credit cannot be frozen because most children
18 do not have credit information or reports.¹²

19 27. For these reasons and others, “[c]hild identity theft is a growing problem in the United
20

21
22 ⁸ Zynga Inc., Form 10-K, Fiscal Year Ended December 31, 2019, found at
<https://investor.zynga.com/static-files/d91122ee-c93f-468b-a48e-6d3b3c1441e3> (last visited 7/27/20).

23 ⁹ “Facebook knowingly duped game-playing kids and their parents out of money,” (1/24/19), found at
24 <https://www.revealnews.org/article/facebook-knowingly-duped-game-playing-kids-and-their-parents-out-of-money/> (last visited 7/27/20).

25 ¹⁰ *Id.*

26 ¹¹ “Documents Show Facebook Knowingly Took Money from Unwitting Children,” (1/25/19), found
at <https://www.popularmechanics.com/technology/apps/a26041842/documents-show-facebook-knowingly-took-money-from-unwitting-children/> (last visited 7/27/20).

27 ¹² “Identity Theft Poses Extra Troubles for Children,” (4/17/15), found at
28 <https://www.nytimes.com/2015/04/18/your-money/a-childs-vulnerability-to-identity-theft.html?searchResultPosition=1> (last visited 7/27/20).

1 States.”¹³

2 **C. With only non-existent or outdated encryption systems in place to protect customer**
 3 **PII, the PII of Plaintiff and the Class were stolen from Zynga.**

4 28. On September 29, 2019, *The Hacker News* reported that a serial hacker from Pakistan
 5 called “Gnosticplayers” breached Zynga’s *Words with Friends* and improperly accessed a “massive
 6 database” of more than 218 million users. The hacker reported that the breach affected all Android
 7 and iOS game players who had installed and signed up for the *Words with Friends* game on or before
 8 September 2, 2019. The information stolen included names, email addresses, login IDs, passwords,
 9 password reset tokens, phone numbers, Facebook IDs and Zynga account IDs.¹⁴

10 29. The Zynga account passwords for those games were secured with SHA-1 cyrptography,
 11 which is an encryption method that “has been considered outdated and insecure since before Zynga
 12 was even founded.”¹⁵ SHA-1, or Secure Hash Algorithm 1, “dates back to 1995 and has been known
 13 to be vulnerable to theoretical attacks since 2005. The U.S. National Institute of Standards and
 14 Technology has banned the use of SHA-1 by U.S. federal agencies since 2010, and digital certificate
 15 authorities have not been allowed to issue SHA-1-signed certificates since Jan. 1, 2016....”¹⁶

16 30. Other Zynga account passwords for different Zynga games were stored in plain text, and
 17 the hacker claimed to have accessed additional data which included clear text passwords for more
 18 than 7 million users.¹⁷

19 31. That millions of passwords were maintained in plain text and others in SHA-1 confirms
 20

21 ¹³ “Never Too Young to Have Your Identity Stolen,” (7/21/07), found at
 22 <https://www.nytimes.com/2007/07/21/business/21idtheft.html?searchResultPosition=2> (last visited
 7/27/20).

23 ¹⁴ “Exclusive — Hacker Steals Over 218 Million Zynga 'Words with Friends' Gamers Data”
 24 (9/29/19), found at <https://thehackernews.com/2019/09/zynga-game-hacking.html> (last visited
 7/27/20).

25 ¹⁵ “Password Breach of Game Developer Zynga Compromises 170 Million Accounts” (12/30/19),
 found at [https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-](https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/)
 26 [compromises-170-million-accounts/](https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/) (last visited 7/27/20).

27 ¹⁶ “The SHA1 hash function is now completely unsafe,” (2/23/17), found at
[https://www.computerworld.com/article/3173616/the-sha1-hash-function-is-now-completely-](https://www.computerworld.com/article/3173616/the-sha1-hash-function-is-now-completely-unsafe.html)
 28 [unsafe.html](https://www.computerworld.com/article/3173616/the-sha1-hash-function-is-now-completely-unsafe.html) (last visited 7/27/20).

¹⁷ “Password Breach of Game Developer Zynga Compromises 170 Million Accounts,” *supra*.

1 that Zynga had inadequate security measures in place to protect and store its users' PII.

2 32. Industry watchers have speculated that it is possible that all of Zynga's accounts dating
3 back to the launch of each game accessed by the hacker have been compromised.¹⁸

4 33. Zynga knew it was vulnerable to such attacks. As early as 2012, in a Securities and
5 Exchange Commission ("SEC") filing, Zynga reported prior hacking attacks and acknowledged that it
6 "will continue to experience hacking attacks." Zynga recognized that it was "a particularly attractive
7 target for hackers," because of its prominence in the social gaming industry. It reported that it had
8 previously been the subject of "civil claims alleging liability for the breach of data privacy."¹⁹

9 34. The Hacker Gnosticplayers, responsible for the recent Zynga attack, is undoubtedly a
10 thief. Gnosticplayers "is a known quantity in the digital criminal underground, having been observed
11 selling hundreds of millions of breached accounts on the dark web since early 2019."²⁰
12 Gnosticplayers had also claimed responsibility for two previous hacking incidents of other websites,
13 one in February, 2019 and the second in March, 2019, where the hacker put information for millions
14 of accounts for sale on the dark web.²¹ "It should be assumed that all of these stolen passwords [from
15 the Zynga Data Breach] will be available in the wild at some point, if they are not already."²²

16 35. All told, the Zynga Data Breach exposed the information of over 170 million of Zynga's
17 customers. According to the website haveibeenpwned.com, the Zynga Data Breach is the tenth
18 largest of all time.²³

19 ¹⁸ *Id.*

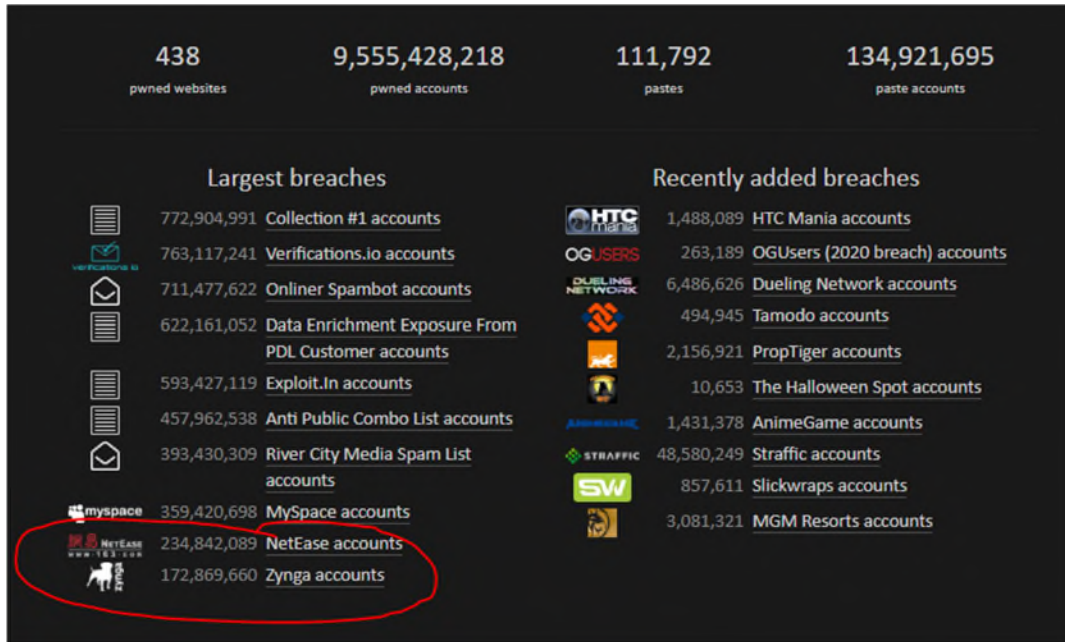
20 ¹⁹ Zynga Inc., Form 10-K, Fiscal Year Ended December 31, 2012, found at
21 <https://www.sec.gov/Archives/edgar/data/1439404/000119312513072858/d489727d10k.htm> (last
22 visited 7/27/20).

23 ²⁰ "Password Breach of Game Developer Zynga Compromises 170 Million Accounts," *supra.*

24 ²¹ <https://thehackernews.com/2019/09/zynga-game-hacking.html>, *supra.* See also "Times when
25 'Gnosticplayers' hacker made headlines for selling troves of stolen data on dark web," (9/30/19),
26 found at <https://cyware.com/news/times-when-gnosticplayers-hacker-made-headlines-for-selling-troves-of-stolen-data-on-dark-web-f8849502> ("Zynga Inc., and American social game developer is the
27 latest victim of 'Gnosticplayers' hacker") (last visited 7/27/20).

28 ²² "Password Breach of Game Developer Zynga Compromises 170 Million Accounts," *supra.*

²³ <https://haveibeenpwned.com/> (last visited 7/27/20). The website haveibeenpwned.com is a free
online resource for an individual to assess if they may have been put at risk due to an online account
having been compromised or "pwned" in a data breach. See also
<https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga->



D. Zynga has failed to adequately notify and protect its customers since learning of the data breach.

36. Zynga admitted that it had been breached in a September 12, 2019, statement posted on its website which it called a “Player Security Announcement.” But Zynga did not accept responsibility for the attack and minimized its scope. Zynga suggested that hacking is unavoidable: “Cyber attacks are one of the unfortunate realities of doing business today. We recently discovered that certain player account information may have been illegally accessed by outside hackers.”²⁴

37. Zynga stated, “we do not believe any financial information was accessed. However, we have identified account login information for certain players of *Draw Something* and *Words with Friends* that may have been accessed.”²⁵

compromises-170-million-accounts/, *supra* (“The amount of account records compromised would make this the 10th largest data breach of all time”).

²⁴ <https://investor.zynga.com/news-releases/news-release-details/player-security-announcement> (last visited 7/27/20).

²⁵ *Id.*

Player Security Announcement

Sep 12, 2019

 PDF Version

Cyber attacks are one of the unfortunate realities of doing business today. We recently discovered that certain player account information may have been illegally accessed by outside hackers. An investigation was immediately commenced, leading third-party forensics firms were retained to assist, and we have contacted law enforcement.

While the investigation is ongoing, we do not believe any financial information was accessed. However, we have identified account login information for certain players of *Draw Something* and *Words With Friends* that may have been accessed. As a precaution, we have taken steps to protect these users' accounts from invalid logins. We plan to further notify players as the investigation proceeds.

The security of our player data is extremely important to us. We are working hard to address this matter and remain committed to supporting our community. Additional information is available on our [Player Support](#) page.

As it relates to our business outlook, we are reaffirming our Third Quarter and Full-Year 2019 guidance and financial outlook as communicated in our [Q2 2019 Quarterly Earnings Letter](#) on July 31, 2019.

38. Zynga's website announcement – had its customers by chance discovered it – failed to offer its customers resources to manage the fraud and was devoid of any suggestions or instructions about protecting their identities and PII from fraud, such as imposing credit freezes, monitoring credit reports, and checking credit card statements. Instead, Zynga's concern lay with its earnings projections as it concluded its announcement by reaffirming the contents of its "Q2 2019 Quarterly Earnings Letter" dated July 31, 2019.²⁶

39. Zynga appears to have discovered the hacking close in time to when it occurred and before the hacking was reported in *The Hacker News*. And while Zynga's website announcement admitted "we have identified account login information for certain players of *Draw Something* and *Words with Friends* that may have been accessed," Zynga never notified those customers by email, or even by a pop-up notification in its gaming applications, so that those customers would be aware of the breach and take timely steps to protect their identities. Instead, it stated that it "plan[s] to further notify players as the investigation proceeds."

40. The only alerts some customers may have received came from third-party haveibeenpwned.com, had those customers had the foresight to sign up for automatic notifications from haveibeenpwned.com. Those alerts were sent on December 18, 2019, three months after Zynga itself was aware of the breach.

41. On that same day, December 18, 2019, whether by design or by coincidence, Zynga modified both its Privacy Policy and Terms of Service.

²⁶ *Id.*

1 42. An industry expert opined, “The disclosure of the full scale and nature of this breach,
2 some three months after the initial announcement, is concerning. This delay, and the initial lack of
3 information provided by Zynga to its users, has put victims at unnecessary risk.”²⁷

4 43. Even to this day there may be millions of individuals who do not realize that their PII
5 was stolen as result of the Zynga Data Breach.

6 44. One primary concern of the Zynga Data Breach is the use of the username and password
7 combinations in credential stuffing attacks.²⁸ “Credential stuffing” is when an cyber attacker takes a
8 massive trove of usernames and passwords from a data breach and tries to “stuff” those credentials
9 into the login page of other digital services. Because people frequently use the same username and
10 password across multiple sites, attackers can often use one piece of credential information to unlock
11 multiple accounts.²⁹

12 45. “Compromised pairs of emails and passwords could be injected into commercial
13 websites like Amazon and Ebay in order to fraudulently gain access. The vast majority of email and
14 password combos won’t work, but a few will. That’s because many people reuse the same credentials
15 on multiple websites.”³⁰

16 46. But credential stuffing is not the only concern of the Zynga Data Breach. The breach
17 also provides enough information for hackers to potentially create targeted phishing attacks made up
18 to look as if they are an official communication from Zynga.³¹

19 47. In addition, because some customers have their games connected to their Facebook
20 accounts, hackers can gain access to far more information to create a forged identity. “Logging in
21 with this stolen information (including the 7 million *Draw Something* passwords left in clear text with
22

23 ²⁷ [https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-](https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/)
24 [compromises-170-million-accounts/](https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/), *supra* (quoting Oz Alashe, CEO of CybSafe, a cyber security
25 awareness platform and cloud data analytics platform).

26 ²⁸ *Id.*

27 ²⁹ “Hacker Lexicon: What Is Credential Stuffing?” (2/17/19) found at
28 <https://www.wired.com/story/what-is-credential-stuffing/> (last visited 7/27/20).

³⁰ [https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-](https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/)
27 [compromises-170-million-accounts/](https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/), *supra* (quoting Oz Alashe).

³¹ [https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-](https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/)
28 [compromises-170-million-accounts/](https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/), *supra*.

1 this breach) makes it impossible to determine if the actual account holder is the one logging in.”³²

2 **E. Data breaches, like Zynga’s, cause financial, emotional, and physical harm to the**
 3 **victims, including to Plaintiff and the Class**

4 48. Annual monetary losses for cybercrimes are estimated to range between \$375 billion
 5 and \$575 billion worldwide. In the United States in 2018, there were 3 million identity theft and
 6 fraud complaints filed with the Federal Trade Commission. Of those, 1.4 million were fraud related,
 7 and 25% of those reported that money was lost. The median amount consumer paid in those cases
 8 was \$375.³³

9 49. But direct, monetary losses are not the only damages that victims of identity theft suffer.
 10 According to a Presidential Report on identity theft, victims of identity theft also suffer indirect
 11 financial costs, as well as physical and emotional injuries:

12 In addition to the losses that result when identity thieves fraudulently open
 13 accounts . . . individual victims often suffer indirect financial costs,
 14 including the costs incurred in both civil litigation initiated by creditors
 15 and in overcoming the many obstacles they face in obtaining or retaining
 credit. Victims of non-financial identity theft, for example, health-related
 or criminal record fraud, face other types of harm and frustration.

16 In addition to out-of-pocket expenses that can reach thousands of dollars
 17 for the victims of new account identity theft, and the emotional toll
 18 identity theft can take, some victims have to spend what can be a
 19 considerable amount of time to repair the damage caused by the identity
 20 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 and open new ones, and
 dispute charges with individual creditors.³⁴

21 50. The indirect costs of identity theft take victims away from their everyday lives. They
 22 spend less time on hobbies and vacations, and are forced to take time off of work and spend time
 23 away from their family. In 2016, more than 25% of victims had to borrow money from family and
 24

25 ³² *Id.* (quoting Robert Prigge, President of Jumio, which provides biometric verification services).

26 ³³ “Facts + Statistics: Identity theft and cybercrime,” found at <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (last visited 7/27/20).

27 ³⁴ “The President’s Identity Theft Task Force, Combating Identity Theft, A Strategic Plan” (April
 28 2007), p.11, found at <https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf> (last visited 7/27/20).

1 friends.³⁵

2 51. The emotional toll that identity theft can take can be grave. Victims suffer from
3 annoyance and frustration, fear of their financial future and financial security, and feel vulnerable,
4 powerless, and helpless. Some seek professional help, and some feel suicidal.³⁶

5 52. “Identity theft can be more than a hassle - replacing credit cards, closing bank accounts,
6 or changing passwords. But for some victims, it can be a life-altering experience that also causes
7 serious emotional problems and can even drive some to consider suicide.”³⁷

8 53. There are also physical side-effects that victims of identity theft suffer. Individuals are
9 unable to concentrate or focus, and suffer from fatigue, sleep disturbances, stress, loss of appetite, and
10 an inability to work because of physical symptoms.³⁸

11 54. The physical and emotional responses caused by identity theft can exist for years at a
12 time. According to the U.S. Government Accountability Office, which conducted a study regarding
13 data breaches, use of stolen data can occur years into the future:

14 [L]aw enforcement officials told us that in some cases, stolen data may be
15 held for up to a year or more before being used to commit identity theft.
16 Further, once stolen data have been sold or posted on the Web, fraudulent
17 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.³⁹

18 55. Plaintiff and the Class had their PII stolen in the Zynga Data Breach, causing Plaintiff
19 and the Class to suffer injuries and damages, including but not limited to the improper disclosure of
20 PII, the loss of value of the PII, disclosure and dissemination of the PII, the actual and imminent threat
21 of identity theft and other fraud, the loss of privacy, and out-of-pocket expense and time devoted to
22

23 ³⁵“Identity Theft: The Aftermath 2017,” p.7, found at https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited 7/27/20).

24 ³⁶ *Id.*

25 ³⁷ “Not Just a Financial Toll: Some Victims of Identity Theft Consider Suicide” (11/6/17), found at
<https://www.nbcnews.com/business/consumer/not-just-financial-toll-some-victims-identity-theft-consider-suicide-n817966> (last visited 7/27/20).

26 ³⁸ “Identity Theft: The Aftermath 2017,” *supra*, p.12.

27 ³⁹ “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, The
28 Full Extent Is Unknown” GAO Report (June 2007), p.29, found at
<https://www.gao.gov/assets/270/262899.pdf> (last visited 7/27/20).

1 mitigating the effects of the data breach.

2 VI. CLASS ACTION ALLEGATIONS

3 56. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, Plaintiff seeks
4 certification of the following Nationwide Class: “All persons residing in the United States whose PII
5 was compromised in the Zynga Inc., data breach that occurred in or around September, 2019, who
6 created a Zynga account prior to August 11, 2014, and who otherwise did not play Zynga’s games
7 after August 10, 2014.”

8 57. **Numerosity: Federal Rule of Civil Procedure 23(a)(1).** The members of the Classes are
9 so numerous and geographically dispersed that individual joinder of all Class members is
10 impracticable. Over 172 million Zynga accounts in the United States and globally have been exposed,
11 making joinder impracticable. Those individuals’ names and addresses are available from
12 Defendant’s records, and Class members may be notified of the pendency of this action by
13 recognized, Court-approved notice dissemination methods.

14 58. **Commonality and Predominance: Federal Rules of Civil Procedure 23(a)(2) and**
15 **23(b)(3).** This action involves common questions of law and fact, which predominate over any
16 questions affecting individual Class members, including:

- 17 a Whether Defendant knew or should have known that its computer and data
18 systems were vulnerable to attack;
- 19 b. Whether Defendant failed to take adequate and reasonable measures to ensure its
20 computer and data systems were protected;
- 21 c. Whether Defendant failed to take available steps to prevent and stop the breach
22 from happening;
- 23 d. Whether Defendant failed to disclose the material facts that it did not have
24 adequate security practices and systems to safeguard its customers’ PII;
- 25 e. Whether Defendant failed to provide timely and adequate notice of the data
26 breach;
- 27 f. Whether Defendant owed a duty to Plaintiff and Class members to protect their
28

1 PII and to provide timely and accurate notice of the data breach to Plaintiff and
2 Class members;

3 g. Whether Defendant breached its duties to protect the PII of Plaintiff and Class
4 members by failing to provide adequate security and by failing to provide timely
5 and accurate notice to Plaintiff and Class members of the data breach;

6 h. Whether Defendant's actions or inactions resulted in or was the proximate cause
7 of the breach of its systems, resulting in the unauthorized access and/or theft of
8 Plaintiff and Class members' PII;

9 i. Whether Defendant's conduct violated state consumer protection laws;

10 j. Whether Defendant's conduct renders it liable for negligence, negligence per se,
11 breach of contract, breach of implied contract, unjust enrichment, and breach of
12 confidence;

13 k. Whether, as a result of Defendant's conduct, Plaintiff and Class members face a
14 significant threat of harm and/or have already suffered harm, and, if so, the
15 appropriate measure of damages to which they are entitled;

16 l. Whether, as a result of Defendant's conduct, Plaintiff and Class members are
17 entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the
18 nature of such relief; and

19 m. Whether, as a result of Defendant's conduct, Plaintiff and Class members are
20 entitled to damages, punitive damages, costs, and attorneys' fees.

21 59. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of
22 other Class members' claims because Plaintiff and Class members were subjected to the same
23 allegedly unlawful conduct and damaged in the same way.

24 60. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an
25 adequate class representative because his interests do not conflict with the interests of Class members
26 who they seeks to represent, Plaintiff has retained counsel competent and experienced in complex
27 class action litigation, and Plaintiff intends to prosecute this action vigorously. The Class members'
28

1 interests will be fairly and adequately protected by Plaintiff and his counsel.

2 61. ***Declaratory and Injunctive Relief: Federal Rule of Civil Procedure 23(b)(2).***

3 Defendant has acted and/or refused to act on grounds generally applicable to the Class, making final
4 injunctive relief or corresponding declaratory relief appropriate.

5 62. ***Superiority: Federal Rule of Civil Procedure 23(b)(3).*** A class action is superior to any
6 other available means for the fair and efficient adjudication of this controversy, and no unusual
7 difficulties are likely to be encountered in the management of this class action. The damages or other
8 financial detriment suffered by Plaintiff and Class members are relatively small compared to the
9 burden and expense that would be required to individually litigate their claims against Defendant, so it
10 would be impracticable for Class members to individually seek redress for Defendant's wrongful
11 conduct. Even if Class members could afford litigation, the court system could not. Individualized
12 litigation creates a potential for inconsistent or contradictory judgments and increases the delay and
13 expense to all parties and the court system. By contrast, the class action device presents far fewer
14 management difficulties and provides the benefits of single adjudication, economies of scale, and
15 comprehensive supervision by a single court, especially where there are over 172 million Zynga users
16 affected.

17 **VII. CLAIMS**

18 **COUNT I - NEGLIGENCE**

19 **(on Behalf of Plaintiff and the Nationwide Class)**

20 63. Plaintiff realleges and incorporates the foregoing allegations as if fully set forth herein.

21 64. Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in
22 obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from
23 being compromised, lost, stolen, accessed, and misused by unauthorized persons.

24 65. This duty included, among other things:

- 25 a. designing, maintaining, and testing its security systems to ensure that Plaintiff's
- 26 and Class members' PII in its possession was adequately secured and protected;
- 27 b. implementing processes that would detect a breach of its security system in a
- 28 timely manner;

- c. timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks;
- d. maintaining data security measures consistent with current technology and industry standards; and
- e. timely notifying customers that their PII had been compromised, lost, stolen, accessed, or misused.

66. Defendant’s duty to use reasonable care arose from several sources. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices.

67. Not only was it foreseeable that Plaintiff and Class Members would be harmed by the Defendant’s failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Defendant knew that it was more likely than not Plaintiff and other Class members would be harmed. Defendant said as much in SEC filings.

68. Defendant’s duty to Plaintiff and Class members also arose because of a special relationship that existed between Defendant and Plaintiff and Class members. That special relationship arose because Plaintiff and the Class member entrusted Defendant with their PII as part of the creation of user accounts necessary to access Zynga’s online and mobile gaming applications. Defendant could have ensured that its security systems and data protection measures were sufficient to minimize or prevent the data breach.

69. Defendant’s duty to Plaintiff and Class members also arose under Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the Federal Trade Commission (“FTC”), the unfair practice of failing to use reasonable measures to protect PII by companies such as Defendant. Various FTC publications and data security breach orders further form the basis of Defendant’s duty. In addition, individual states have enacted statutes based upon the FTCA that also created a duty.

70. Defendant breached the duties it owed to Plaintiff and Class members described above

1 and thus was negligent. Defendant breached these duties by, among other things, failing to: (a)
2 exercise reasonable care and implement adequate security systems, protocols and practices sufficient
3 to protect the PII of Plaintiff and Class members; (b) detect the breach while it was ongoing; (c)
4 maintain security systems consistent with current technology and industry standards; and (d) timely
5 disclose that Plaintiff's and Class members' PII in Defendant's possession had been or was
6 reasonably believed to have been, stolen or compromised.

7 71. Timely notification of the data breach was required, appropriate, and necessary so that,
8 among other things, Plaintiff and Class members could take appropriate measures to freeze or lock
9 their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or
10 change usernames and passwords on compromised accounts, monitor their account information and
11 credit reports for fraudulent activity, contact their banks or other financial institutions that issue their
12 credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate
13 the damages caused by Defendant's misconduct.

14 72. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and
15 Class members, their PII would not have been compromised.

16 73. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members
17 have been injured as described herein, and are entitled to damages, including compensatory, punitive,
18 and nominal damages, in an amount to be proven at trial.

19 74. Plaintiff's and Class members' injuries include:

- 20 a theft of their PII;
- 21 b. costs associated with the detection and prevention of identity theft and
22 unauthorized use of their financial accounts;
- 23 c. costs associated with purchasing credit monitoring and identity theft protection
24 services;
- 25 d. unauthorized charges and loss of use of and access to their financial account
26 funds and costs associated with inability to obtain money from their accounts or
27 being limited in the amount of money they were permitted to obtain from their
28

1 accounts, including missed payments on bills and loans, late charges and fees,
2 and adverse effects on their credit;

3 e. lowered credit scores resulting from credit inquiries following fraudulent
4 activities;

5 f. costs associated with time spent and the loss of productivity from taking time to
6 address and attempt to ameliorate, mitigate, and deal with the actual and future
7 consequences of the data breach — including finding fraudulent charges,
8 cancelling and reissuing cards, enrolling in credit monitoring and identity theft
9 protection services, freezing and unfreezing accounts, and imposing withdrawal
10 and purchase limits on compromised accounts;

11 g. the physical and emotional injuries caused by being victimized by a data breach;

12 h. the imminent and certainly impending injury flowing from potential fraud and
13 identify theft posed by their PII being placed in the hands of criminals; and

14 i. continued risk of exposure to hackers and thieves of their PII, which remains in
15 Defendant’s possession and is subject to further breaches so long as Defendant
16 fails to undertake appropriate and adequate measures to protect Plaintiff and
17 Class members.

18 **COUNT II - NEGLIGENCE PER SE**
19 **(on Behalf of Plaintiff and the Nationwide Class)**

20 75. Plaintiff realleges and incorporates the foregoing allegations as if fully set forth herein.

21 76. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits “unfair . . .
22 practices in or affecting commerce” including, as interpreted and enforced by the Federal Trade
23 Commission (“FTCA”), the unfair act or practice by companies such as Defendant of failing to use
24 reasonable measures to protect PII. This statute, and the various related FTCA publications and
25 orders, form the basis of Defendant’s duty to Plaintiff in this negligence per se claim.

26 77. Defendant violated Section 5 of the FTCA (and similar state statutes) by failing to use
27 reasonable measures to protect Plaintiff’s and Class members’ PII, failing to use current and generally
28

1 accepted technology, and not complying with industry standards. Defendant's conduct was
2 particularly unreasonable given the size of its customer database, the nature and amount of PII it
3 obtained and stored, and the foreseeable consequences of a data breach.

4 78. Defendant's violation of Section 5 of the FTCA (and similar state statutes) constitutes
5 negligence per se.

6 79. Plaintiff and Class members are not seeking to hold Defendant liable under the FTCA,
7 itself. Instead, that section forms the basis of Defendants' duty to Plaintiff and Class members.

8 80. Class members are consumers within the class of persons Section 5 of the FTCA (and
9 similar state statutes) was intended to protect.

10 81. Moreover, the harm that has occurred is the type of harm the FTCA (and similar state
11 statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions
12 against businesses which, as a result of their failure to employ reasonable data security measures and
13 avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class.

14 82. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members
15 have been injured as described herein, and are entitled to damages, including compensatory, punitive,
16 and nominal damages, in an amount to be proven at trial.

17 **COUNT III - BREACH OF CONTRACT**
18 **(on Behalf of Plaintiff and the Nationwide Class)**

19 83. Plaintiff realleges and incorporates the foregoing allegations as if fully set forth herein.

20 84. Zynga's Privacy Policy (the "Privacy Policy") is an agreement between Zynga and
21 persons who provide their PII to Zynga, including Plaintiff and Class members.

22 85. Based upon information and belief, the Privacy Policy, as it was in effect at the time of
23 the Zynga Data Breach, promised that "[w]e implement reasonable and appropriate security measures
24 to help protect the security of your information both online and offline and to ensure that your data is
25 treated securely."

26 86. The Privacy Policy, as it was in effect at the time of the Zynga Data Breach, stated that
27 it applies to persons who use Zynga's services, meaning games, products, services, content,
28

1 Zynga.com, and/or domain or website operated by Zynga, and it details how Zynga will both protect
2 and use the PII provided by users of Zynga's services.

3 87. Plaintiff and Class members on the one hand and Zynga on the other formed a contract
4 when Plaintiff and Class members provided PII to Zynga subject to the Privacy Policy and used
5 Zynga's services.

6 88. Plaintiff and Class members fully performed their obligations under the contract with
7 Zynga.

8 89. Zynga breached its agreement with Plaintiff and Class members by failing to protect
9 their PII. Specifically, Defendant (1) failed to use reasonable measures to protect that information;
10 and (2) disclosed that information to unauthorized third parties, in violation of the agreement.

11 90. As a direct and proximate result of these breaches of contract, Plaintiff and Class
12 members sustained actual losses and damages as described in detail above, including but not limited
13 to being denied the benefit of the bargain pursuant to which they provided their PII to Zynga.

14 **COUNT IV - BREACH OF IMPLIED CONTRACT**
15 **(on Behalf of Plaintiff and the Nationwide Class)**

16 91. Plaintiff realleges and incorporates the foregoing allegations as if fully set forth herein.

17 92. This claim is an alternative to Plaintiff's and the Nationwide Class' breach of contract
18 claim.

19 93. Plaintiff and Class members alternatively entered into an implied contract with Zynga
20 when they obtained services from Zynga, or otherwise provided PII to Zynga.

21 94. As part of these transactions, Zynga agreed to safeguard and protect the PII of Plaintiff
22 and Class members.

23 95. Plaintiff and Class members entered into implied contracts with the reasonable
24 expectation that Zynga's data security practices and policies were reasonable and consistent with
25 industry standards. Under the implied contracts, Plaintiff and Class members believed that Defendant
26 would use part of the monies paid to Zynga or monies it derived from advertising to provide
27 reasonable and adequate data security to protect Plaintiff's and Class members' PII.
28

1 105. But for Defendant’s willingness and commitment to maintain its privacy and
2 confidentiality, Plaintiff and Class members would not have provided their PII to the Defendant.

3 106. Defendant continues to benefit and profit from its retention and use of the PII while its
4 value to Plaintiff and Class members has been diminished.

5 107. Defendant benefitted by Plaintiff and Class members’ purchases of mobile gaming
6 applications or in-game items, or using Defendant’s free gaming applications where paid advertising
7 was displayed, and this benefit was more than those services were worth to Plaintiff and Class
8 members had been aware that Defendant would fail to protect their PII.

9 108. Zynga also benefitted through its unjust conduct by retaining money that it should have
10 used to provide reasonable and adequate data security to protect Plaintiff’s and Class members’ PII.

11 109. It is inequitable for Defendant to retain these benefits.

12 110. As a result of Defendant’s wrongful conduct including, among other conduct, its
13 knowing failure to employ adequate data security measures, its continued maintenance and use
14 Plaintiff’s and Class members’ PII without having adequate data security measures, and its other
15 conduct facilitating the theft of that PII, Defendant has been unjustly enriched at the expense of, and
16 to the detriment of, Plaintiff and Class members.

17 111. Defendant’s unjust enrichment is traceable to, and resulted directly and proximately
18 from, the conduct alleged herein, including the compiling and use of Plaintiff’s and Class members’
19 PII, while at the same time failing to maintain that information secure from intrusion and theft by
20 hackers and thieves.

21 112. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to
22 be permitted to retain the benefits it received, and is still receiving, without justification, from
23 Plaintiff and Class members in an unfair and unconscionable manner. Defendant’s retention of such
24 benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

25 113. The benefits conferred upon, received, and enjoyed by Defendant were not conferred
26 officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain these
27 benefits.

1 114. Plaintiff and Class members have no adequate remedy at law.

2 115. Defendant is therefore liable to Plaintiff and Class members for restitution or
3 disgorgement in the amount of the benefit conferred on Defendant as a result of its wrongful conduct,
4 including specifically: the value to Defendant of the PII that was stolen in the Zynga Data Breach; the
5 profits Defendant is receiving from the use of that information; the amount that Zynga overcharged
6 Plaintiff and Class members for use of its online and mobile gaming application services through in-
7 app purchases; and the amounts that Zynga should have spent to provide reasonable and adequate data
8 security to protect Plaintiff's and Class members' PII.

9 **COUNT VI - BREACH OF CONFIDENCE**
10 **(on Behalf of Plaintiff and the Nationwide Class)**

11 116. Plaintiff realleges and incorporates the foregoing allegations as if fully set forth herein.

12 117. At all times, Defendant was aware of the confidential and sensitive nature of Plaintiff's
13 and Class members' PII.

14 118. As alleged herein and above, Zynga's relationship with Plaintiff and Class members was
15 governed by terms of the Privacy Policy and/or the implied expectation that Plaintiff's and Class
16 members' PII would be collected, stored, and protected in confidence, and would not be disclosed to
17 the public or any unauthorized third parties.

18 119. Plaintiff's and Class members provided their PII to Zynga with the explicit and implicit
19 understandings that Defendant would protect and not permit the PII to be disseminated to the public or
20 any unauthorized parties.

21 120. Plaintiff and Class members also provided their respective PII to Zynga with the explicit
22 and implicit understandings that Defendant would take precautions to protect the PII from unauthorized
23 disclosure, such as following basic principles of encryption and information security practices.

24 121. Zynga voluntarily received in confidence Plaintiff's and Class members' PII with the
25 understanding that PII would not be disclosed or disseminated to the public or any unauthorized third
26 parties.

27 122. Due to Zynga's failure to prevent, detect, avoid the data breach from occurring by
28

1 following best systems and security practices to secure Plaintiff's and Class members' PII, Plaintiff's
2 and Class members' PII was disclosed and misappropriated to unauthorized third parties and the public
3 beyond Plaintiff's and Class members' confidence, and without their express permission.

4 123. But for Defendant's disclosure of Plaintiff's and Class members' PII in violation of the
5 parties' understanding of confidence, their PII would not have been compromised, stolen, viewed,
6 accessed, and used by unauthorized third parties. The Zynga Data Breach was the direct and legal cause
7 of the theft of Plaintiff's and Class members' PII, as well as the resulting damages.

8 124. The injury and harm Plaintiff and Class members suffered was the reasonably foreseeable
9 result of Defendant's unauthorized disclosure of Plaintiff's and Class members' PII. Zynga knew its
10 computer systems for accepting, securing, and storing Plaintiff's and Class members' PII had serious
11 security vulnerabilities where Zynga failed to observe even basic information security practices or
12 correct known security vulnerabilities.

13 125. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and
14 Class members have been injured as described herein, and are entitled to damages, including
15 compensatory, punitive, and nominal damages, in an amount to be proven at trial.

16
17 **COUNT VII - VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW**
18 **CAL. BUS. & PROF. CODE, §§ 17200, ET SEQ.**
(on Behalf of Plaintiff and the Nationwide Class)

19 126. Plaintiff realleges and incorporates the foregoing allegations as if fully set forth herein.

20 127. Defendant violated the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof.
21 Code §§ 17200, et seq., by engaging in unlawful, unfair, and deceptive business acts and practices.

22 128. Defendant is a "person" as defined by Cal. Bus. & Prof. Code §17201.

23 129. Defendant's unlawful, unfair, and deceptive acts and practices include:

- 24 a. Failing to implement and maintain reasonable security measures to protect
25 Plaintiff's and Class members' PII from unauthorized disclosure, release, data
26 breaches, and theft, which was a direct and proximate cause of the data breach.
27 b. Failing to identify foreseeable security and privacy risks, remediate identified
28

1 security and privacy risks, and adequately improve security and privacy measures
2 despite knowing the risk of cybersecurity incidents, which was a direct and
3 proximate cause of the data breach. This conduct was unfair when weighed
4 against the harm to Plaintiff and Class members, whose PII has been
5 compromised;

- 6 c. Failing to implement and maintain reasonable security measures, which was
7 contrary to legislatively declared public policy that seeks to protect consumers'
8 data and ensure that entities that are trusted with it use appropriate security
9 measures. These policies are reflected in laws, including the FTCA, 15 U.S.C. §
10 45, and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5;
- 11 d. Failing to comply with common law and statutory duties pertaining to the
12 security and privacy of Plaintiff's and Class members' PII, including duties
13 imposed by the FTCA, 15 U.S.C. § 45 and California's Customer Records Act,
14 Cal. Civ. Code §§ 1798.80, et seq., which was a direct and proximate cause of
15 the data breach;
- 16 e. Failing to implement and maintain reasonable security measures, which led to
17 substantial injuries, as described above, that are not outweighed by any
18 countervailing benefits to consumers or competition. Moreover, because
19 consumers could not know of Defendant's inadequate security, consumers could
20 not have reasonably avoided the harms that Defendant caused;
- 21 f. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82,
22 by failing to disclose a data security breach and failing to notify or timely notify
23 Plaintiff and Class members that their PII had been accessed and stolen;
- 24 g. Misrepresenting in its Privacy Policy and elsewhere that it would protect the
25 privacy and confidentiality of Plaintiff's and Class members' PII, including by
26 implementing and maintaining reasonable security measures;
- 27 h. Omitting, suppressing, and concealing the material fact that it did not reasonably
28

1 or adequately secure Plaintiff's and Class members' PII;

- 2 i. Omitting, suppressing, and concealing the material fact that it did not comply
3 with common law and statutory duties pertaining to the security and privacy of
4 Plaintiff's and Class members' PII, including duties imposed by the FTCA, 15
5 U.S.C. § 45 and California's Customer Records Act, Cal. Civ. Code §§ 1798.80,
6 et seq.; and
7 j. Failing to notify Plaintiff and Class members that their PII had been accessed and
8 stolen.

9 130. Defendant has also engaged in "unlawful" business practices by violating multiple laws,
10 including California's Customer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data
11 security measures) and 1798.82 (requiring timely breach notification), California False Advertising
12 Law, Cal. Bus. & Prof. Code §§ 17500, et seq., California's Consumers Legal Remedies Act, Cal.
13 Civ. Code §§ 1780, et seq., the FTCA, 15 U.S.C. § 45, and California common law.

14 131. Defendant's representations and omissions were material because they were likely to
15 deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect
16 the confidentiality of consumers' PII.

17 132. Defendant had exclusive knowledge of material facts not known to Plaintiff and Class
18 members and Defendant made partial representations but also suppressed some material facts.

19 133. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts
20 and practices, Plaintiff and Class members were injured and lost money or property: the money
21 received by Zynga for its services; the loss of the benefit of their bargain with and overcharges by
22 Zynga as they would not have paid Zynga for services or would have paid less for such services but
23 for the violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and
24 identity protection services; time and expenses related to monitoring their financial accounts for
25 fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity
26 theft.

27 134. Defendant acted intentionally, knowingly, and maliciously to violate California's UCL,
28

1 and recklessly disregarded Plaintiff's and Class members' rights and interests. As disclosed in SEC
 2 filings, Defendant knew that its security and privacy protections were vulnerable to attack, and
 3 Defendant knew that its security measures were inadequate in the face of such attack.

4 135. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law,
 5 including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent
 6 business practices or use of their PII; declaratory relief; injunctive relief; and other appropriate
 7 equitable relief.

8
 9 **COUNT VIII - VIOLATIONS OF THE CALIFORNIA FALSE ADVERTISING LAW**
 10 **CAL. BUS. & PROF. CODE § 17500, ET SEQ.**
 11 **(on Behalf of Plaintiff and the Nationwide Class)**

12 136. Plaintiff incorporates by reference all paragraphs as though fully set forth herein.

13 137. Defendant violated the California False Advertising Law ("FAL"), Cal. Bus. & Prof.
 14 Code §§ 17500, et seq., by engaging in unlawful, untrue, misleading and deceptive advertising and
 15 practices.

16 138. Section 17500 of the Cal. Bus. & Prof. Code states: "It is unlawful for any . . .
 17 corporation . . . with intent directly or indirectly . . . to perform services, professional or otherwise, or
 18 anything of any nature whatsoever or to induce the public to enter into any obligation relating thereto,
 19 to make or disseminate or cause to be made or disseminated before the public in this state, or to make
 20 or disseminate or cause to be made or disseminated from this state before the public in any state, in
 21 any newspaper or other publication, or any advertising device, . . . or in any other manner or means
 22 whatever, including over the Internet, any statement, concerning that real or personal property or
 23 those services, professional or otherwise, or concerning any circumstance or matter of fact connected
 24 with the proposed performance or disposition thereof, which is untrue or misleading, and which is
 25 known, or which by the exercise of reasonable care should be known, to be untrue or misleading. . . ."

26 139. Defendant caused to be made or disseminated through California and the United States,
 27 through advertising, marketing and other publications, the following statements or omissions that
 28 were untrue or misleading, and which were known, or which by the exercise of reasonable care should

1 have been known to Defendant, to be untrue and misleading to consumers, including Plaintiff and the
2 other Class members:

- 3 a Failing to disclose that reasonable security measures to protect Plaintiff's and
4 Class members' PII from unauthorized disclosure, release, data breaches, and
5 theft, were in place, which was a direct and proximate cause of the data breach.
- 6 b. Failing to disclose foreseeable security and privacy risks, remediate identified
7 security and privacy risks, and adequately improve security and privacy measures
8 despite knowing the risk of cybersecurity incidents, which was a direct and
9 proximate cause of the data breach. This conduct was unfair when weighed
10 against the harm to Plaintiff and Class members, whose PII has been
11 compromised;
- 12 c. Failing to disclose non-compliance with reasonable security measures, which was
13 contrary to legislatively declared public policy that seeks to protect consumers'
14 data and ensure that entities that are trusted with it use appropriate security
15 measures. These policies are reflected in laws, including the FTCA, 15 U.S.C. §
16 45, and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5;
- 17 d. Failing to disclose non-compliance with common law and statutory duties
18 pertaining to the security and privacy of Plaintiff's and Class members' PII,
19 including duties imposed by the FTCA, 15 U.S.C. § 45 and California's
20 Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., which was a direct
21 and proximate cause of the data breach;
- 22 e. Failing to disclose non-compliance with reasonable security measures, which led
23 to substantial injuries, as described above, that are not outweighed by any
24 countervailing benefits to consumers or competition. Moreover, because
25 consumers could not know of Defendant's inadequate security, consumers could
26 not have reasonably avoided the harms that Defendant caused;
- 27 f. Failing to disclose a data security breach in violation of Cal. Civ. Code §
28

1 1798.82, and failing to notify or timely notify Plaintiff and Class members that
2 their PII had been accessed and stolen;

3 g Misrepresenting in its Privacy Policy and elsewhere that it would protect the
4 privacy and confidentiality of Plaintiff's and Class members' PII, including by
5 implementing and maintaining reasonable security measures;

6 h Omitting, suppressing, and concealing the material fact that it did not reasonably
7 or adequately secure Plaintiff's and Class members' PII; and

8 i Omitting, suppressing, and concealing the material fact that it did not comply
9 with common law and statutory duties pertaining to the security and privacy of
10 Plaintiff's and Class members' PII, including duties imposed by the FTCA, 15
11 U.S.C. § 45 and California's Customer Records Act, Cal. Civ. Code §§ 1798.80,
12 et seq..

13 140. Defendant violated § 17500 because the misrepresentations and omissions identified
14 above induced Plaintiff and the Class to provide their PII to Defendant, and were therefore material
15 and likely to deceive a reasonable consumer.

16 141. Plaintiff and Class members have suffered an injury in fact, including the loss of money
17 or property, as a result of Defendant's unlawful, untrue, misleading and deceptive advertising and
18 practices.

19 142. Defendant's representations and omissions were material because they were likely to
20 deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect
21 the confidentiality of consumers' PII.

22 143. Defendant had exclusive knowledge of material facts not known to Plaintiff and Class
23 members and Defendant made partial representations but also suppressed some material facts.

24 144. As a direct and proximate result of Defendant's unlawful, untrue, misleading and
25 deceptive advertising and practices, Plaintiff and Class members were injured and lost money or
26 property: the money received by Zynga for its services; the loss of the benefit of their bargain with
27 and overcharges by Zynga as they would not have paid Zynga for services or would have paid less for
28

1 such services but for the violations alleged herein; losses from fraud and identity theft; costs for credit
2 monitoring and identity protection services; time and expenses related to monitoring their financial
3 accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud
4 and identity theft.

5 145. All of the wrongful conduct alleged herein occurred, and continues to occur, in the
6 conduct of Defendant’s business.

7 146. Defendant’s wrongful conduct is part of a pattern or generalized course of conduct that
8 is still perpetuated and repeated, both in the State of California and nationwide.

9 147. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law,
10 including restitution of all profits stemming from Defendant’s unfair, unlawful, and fraudulent
11 business practices or use of their PII; declaratory relief; injunctive relief; and other appropriate
12 equitable relief.

13 **COUNT IX - VIOLATIONS OF THE CALIFORNIA CONSUMERS LEGAL REMEDIES**
14 **ACT,**
15 **CAL. CIV. CODE § 1750, ET SEQ.**
16 **(on Behalf of Plaintiff and the Nationwide Class)**

17 148. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set
18 forth herein.

19 149. Defendant violated the California Consumers Legal Remedies Act (“CLRA”), Cal. Civ.
20 Code §§ 1750, et seq., by engaging in unlawful, untrue, misleading and deceptive advertising and
21 practices.

22 150. Section 1750 of the California Civil Code provides that certain “unfair methods of
23 competition and unfair or deceptive acts or practices undertaken by any person in a transaction
24 intended to result or that results in the sale or lease of goods or services to any consumer are
25 unlawful...” Such practices include “[r]epresenting that goods or services have sponsorship,
26 approval, characteristics, ingredients, uses, benefits, or quantities that they do not have...” and
27 “[r]epresenting that goods or services are of a particular standard, quality, or grade, or that goods are
28 of a particular style or model, if they are of another....” Cal. Civil Code §1750(a)(5) & (7).

1 151. Defendant misrepresented the nature of their products and services in violation of the
2 CLRA by engaging in unlawful, unfair, and deceptive acts and practices including:

- 3 a. Failing to disclose its failure to implement and maintain reasonable security
4 measures to protect Plaintiff's and Class members' PII from unauthorized
5 disclosure, release, data breaches, and theft, which was a direct and proximate
6 cause of the data breach.
- 7 b. Failing to identify foreseeable security and privacy risks, remediate identified
8 security and privacy risks, and adequately improve security and privacy measures
9 despite knowing the risk of cybersecurity incidents, which was a direct and
10 proximate cause of the data breach. This conduct was unfair when weighed
11 against the harm to Plaintiff and Class members, whose PII has been
12 compromised;
- 13 c. Failing to disclose its failure to implement and maintain reasonable security
14 measures, which was contrary to legislatively declared public policy that seeks to
15 protect consumers' data and ensure that entities that are trusted with it use
16 appropriate security measures. These policies are reflected in laws, including the
17 FTCA, 15 U.S.C. § 45, and California's Consumer Records Act, Cal. Civ. Code
18 § 1798.81.5;
- 19 d. Failing to comply with common law and statutory duties pertaining to the
20 security and privacy of Plaintiff's and Class members' PII, including duties
21 imposed by the FTCA, 15 U.S.C. § 45 and California's Customer Records Act,
22 Cal. Civ. Code §§ 1798.80, et seq., which was a direct and proximate cause of
23 the data breach;
- 24 e. Failing to disclose its failure to implement and maintain reasonable security
25 measures, which led to substantial injuries, as described above, that are not
26 outweighed by any countervailing benefits to consumers or competition.
27 Moreover, because consumers could not know of Defendant's inadequate
28

1 security, consumers could not have reasonably avoided the harms that Defendant
2 caused;

3 f. Engaging in unlawful business practices by violating California Civil Code
4 section 1798.82, by failing to disclose a data security breach and failing to notify
5 Plaintiff and Class members that their PII had been accessed and stolen;

6 g. Misrepresenting in its Privacy Policy and elsewhere that it would protect the
7 privacy and confidentiality of Plaintiff's and Class members' PII, including by
8 implementing and maintaining reasonable security measures;

9 h. Omitting, suppressing, and concealing the material fact that it did not reasonably
10 or adequately secure Plaintiff's and Class members' PII;

11 i. Omitting, suppressing, and concealing the material fact that it did not comply
12 with common law and statutory duties pertaining to the security and privacy of
13 Plaintiff's and Class members' PII, including duties imposed by the FTCA, 15
14 U.S.C. § 45 and California's Customer Records Act, Cal. Civ. Code §§ 1798.80,
15 et seq.; and

16 j. Failing to notify or timely notify Plaintiff and Class members that their PII had
17 been accessed and stolen.

18 152. As a direct and proximate result of Defendant's unlawful acts and practices, Plaintiff
19 and Class members were injured and lost money or property: the money received by Zynga for its
20 services; the loss of the benefit of their bargain with and overcharges by Zynga as they would not
21 have paid Zynga for services or would have paid less for such services but for the violations alleged
22 herein; losses from fraud and identity theft; costs for credit monitoring and identity protection
23 services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss
24 of value of their PII; and an increased, imminent risk of fraud and identity theft.

25 153. Defendant acted intentionally, knowingly, and maliciously to violate California's
26 CLRA, and recklessly disregarded Plaintiff's and Class members' rights and interests. As disclosed
27 in SEC filings, Defendant knew that its security and privacy protections were vulnerable to attack, and
28

1 Defendant knew that its security measures were inadequate in the face of such attack.

2 154. Plaintiff and Class members seek injunctive relief, declaratory relief, reasonable
3 attorneys' fees and costs, and other appropriate equitable relief.

4 155. On the same day that this Complaint was filed, Plaintiff has provided Defendant with
5 notice of its violations of the CLRA and a demand on behalf of themselves and the Class pursuant to
6 California Civil Code section 1782(a). If after 30 days, Defendant has not satisfied Plaintiff's demand
7 in whole and on behalf of all Class members, Plaintiff will amend this Complaint to seek all damages
8 stemming from Defendant's unlawful conduct.

9
10 **COUNT X - ALTERNATIVE COUNT FOR VIOLATIONS OF STATE CONSUMER**
11 **PROTECTION ACTS**
12 **(on Behalf of Plaintiff and the Nationwide Class)**

13 156. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set
14 forth herein.

15 157. This claim is an alternative to Plaintiff's and the Nationwide Class' claims under
16 California's UCL, FAL and CLRA, and is brought individually, and on behalf of all similarly situated
17 residents of each of the 50 states for violations of the state consumer protection acts including:

- 18 a the Alaska Unfair Trade Practices and Consumer Protection Act, Alaska Stat. §
19 45.50.471, et seq.;
- 20 b the Arizona Consumer Fraud Act, Ariz. Rev. Stat. §§ 44-1521, et seq.;
- 21 c the Arkansas Deceptive Trade Practices Act, Ark. Code § 4-88-101, et seq.;
- 22 d the California Unfair Competition Law, Bus. & Prof. Code §§ 17200, et seq. and
23 17500, et seq.;
- 24 e the California Consumers Legal Remedies Act, Cal. Civ. Code § 1750, et seq.;
- 25 f the Colorado Consumer Protection Act, Colo. Rev. Stat. Ann. § 6-1-101, et seq.;
- 26 g the Connecticut Unfair Trade Practices Act, Conn. Gen Stat. Ann. § 42- 110, et
27 seq.;
- 28 h the Delaware Consumer Fraud Act, 6 Del. Code § 2513, et seq.;

- 1 i the D.C. Consumer Protection Procedures Act, D.C. Code § 28-3901, et seq.;
- 2 j the Florida Deceptive And Unfair Trade Practices Act, Fla. Stat. Ann. § 501.201,
- 3 et seq.;
- 4 k the Georgia Fair Business Practices Act, Ga. Code Ann. § 10-1-390, et seq.;
- 5 l the Hawaii Unfair Competition Law, Haw. Rev. Stat. § 480-2, et seq.;
- 6 m the Idaho Consumer Protection Act, Idaho Code. Ann. § 48-601, et seq.;
- 7 n the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS
- 8 501/1, et seq.;
- 9 o the Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5-2, et seq.;
- 10 p the Iowa Consumer Fraud Act, Iowa Code § 714H, et seq.;
- 11 q the Kansas Consumer Protection Act, Kan. Stat. Ann. § 50-623, et seq.;
- 12 r the Kentucky Consumer Protection Act, Ky. Rev. Stat. Ann. § 367.110, et seq.;
- 13 s the Louisiana Unfair Trade Practices And Consumer Protection Law, LSA-R.S.
- 14 51:1401, et seq.;
- 15 t the Maine Unfair Trade Practices Act, Me. Rev. Stat. Ann. Tit. 5, § 207, et seq.;
- 16 u the Maryland Consumer Protection Act, Md. Code Ann. Com. Law, § 13-301, et
- 17 seq.;
- 18 v the Massachusetts Regulation of Business Practices for Consumers Protection
- 19 Act, Mass. Gen Laws Ann. Ch. 93A, et seq.;
- 20 w the Michigan Consumer Protection Act, Mich. Comp. Laws Ann. § 445.901, et
- 21 seq.;
- 22 x the Minnesota Prevention of Consumer Fraud Act, Minn. Stat. § 325F, et seq.;
- 23 y the Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407, et seq.;
- 24 z the Nebraska Consumer Protection Act, Neb. Rev. St. §§ 59-1601, et seq.;
- 25 aa the Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. § 41.600, et seq.
- 26 bb the New Hampshire Regulation of Business Practices For Consumer Protection,
- 27 N.H. Rev. Stat. § 358-A:1, et seq.;
- 28

- 1 cc. the New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8, et seq.;
- 2 dd. the New Mexico Unfair Practices Act, N.M. Stat. Ann. § 57-12-1, et seq.;
- 3 ee. the New York Consumer Protection from Deceptive Acts and Practices, N.Y.
- 4 Gen. Bus. Law § 349, et seq.;
- 5 ff. the North Carolina Unfair And Deceptive Trade Practices Act, N.C. Gen Stat. §
- 6 75-1.1, et seq.;
- 7 gg. the North Dakota Consumer Fraud Act, N.D. Cent. Code § 51-15, et seq.;
- 8 hh. the Ohio Consumer Sales Practices Act, Ohio Rev. Code Ann. § 1345.01, et seq.;
- 9 ii. the Oklahoma Consumer Protection Act, Okla. Stat. tit. 15 § 751, et seq.;
- 10 jj. the Oregon Unlawful Trade Practices Act, Or. Rev. Stat. § 646.605, et seq.;
- 11 kk. the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §
- 12 201-1, et seq.;
- 13 ll. the Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1-5.2(B),
- 14 et seq.;
- 15 mm. the South Carolina Unfair Trade Practices Act, S.C. Code Ann. §§ 39-5- 10, et
- 16 seq.;
- 17 mn. the South Dakota Deceptive Trade Practices and Consumer Protection, S.D.
- 18 Codified Laws § 37-24-1, et seq.;
- 19 oo. the Tennessee Consumer Protection Act, Tenn. Code Ann. § 47-18-101, et seq.;
- 20 pp. the Texas Deceptive Trade Practices-Consumer Protection Act, Tex. Code Ann.,
- 21 Bus. & Con. § 17.41, et seq.;
- 22 qq. the Utah Consumer Sales Practices Act, Utah Code. Ann. § 13-11-175, et seq.;
- 23 rr. the Vermont Consumer Fraud Act, 9 V.S.A. § 2451, et seq.;
- 24 ss. the Virginia Consumer Protection Act of 1977, Va. Code Ann. § 59.1-199, et
- 25 seq.;
- 26 tt. the Washington Consumer Protection Act, Wash. Rev. Code § 19.86.010, et seq.;
- 27 uu. the West Virginia Consumer Credit And Protection Act, W. Va. Code § 46A, et
- 28

1 seq.;

2 w. the Wisconsin Deceptive Trade Practices Act, Wis. Stat. § 100.18, et seq.; and

3 w. the Wyoming Consumer Protection Act, Wyo. Stat. Ann. § 40-12-101, et seq.

4 158. The acts, practices, misrepresentations and omissions by Defendant described above,
5 and Defendant's dissemination of deceptive and misleading advertising and marketing materials in
6 connection therewith, occurring in the course of conduct involving trade or commerce, constitute
7 unfair methods of competition and unfair or deceptive acts or practices within the meaning of each of
8 the above-enumerated statutes.

9 159. Defendant's acts and practices described herein misled, deceived or damaged Plaintiff
10 and Class members in connection providing the goods and services mentioned herein. Defendant's
11 conduct also constituted the use or employment of deception, fraud, false pretense, false promise,
12 misrepresentation, or knowingly concealing, suppressing, or omitting a material fact with intent that
13 others rely upon the concealment, suppression or omission in connection with the sale or
14 advertisement of goods or services whether or not a person has in fact been misled, deceived or
15 damaged in violation of each of the above-enumerated statutes.

16 160. Defendants knew or should have known that their conduct violated the above-
17 enumerated statutes. Defendants intended that the Plaintiff and Class members would rely on their
18 misrepresentations, omissions, and concealment of information.

19 161. The foregoing acts, omissions, and practices proximately caused Plaintiff and Class
20 members to suffer damages as described herein.

21 162. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law,
22 including damages stemming from Defendant's unfair, unlawful, and fraudulent business practices or
23 use of their PII; declaratory relief; reasonable attorneys' fees and costs; injunctive relief; and other
24 appropriate equitable relief.

25 163. On April 14, 2020, the Iowa Attorney General approved the filing of this Class Action
26 Complaint after having been provided with a request for approval under Iowa Code 714H.7.

27 164. Plaintiff has provided Defendants with notice of their violations of Code of Ala. § 8-19-
28

10, Alaska Stat. § 45.50.535, Cal. Civ. Code § 1782(a), Ga. Code Ann. § 10-1-399, 815 ILCS 505/10a, Ind. Code Ann. § 24-5-0.5-5, Me. Rev. Stat. Ann. Tit. 5, § 213, Mass. Gen Laws Ann. Ch. 93A, Miss. Code Ann. § 75-24-15, Tex. Bus. & Com. Code § 17.505, W. Va. Code § 46A-6-106, Wyo. Stat. § 40-12-109, and any other state consumer protection statute requiring notice to them of a claim for damages. The notice was transmitted on the day this lawsuit and Amended Complaint were filed. Plaintiff initially brings a claim for injunctive or equitable relief under these particular statutes. After the respective cure periods have expired and Defendants have failed to adequately address the violations alleged herein, Plaintiff will amend the complaint to add a claim for damages under the respective statutes.

WHEREFORE, Plaintiff Christopher Rosiak respectfully requests that this Court:

- a. Certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's counsel as Class Counsel;
- b. Grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;
- c. Award Plaintiff and Class members compensatory, consequential, general, and nominal damages in an amount to be determined at trial;
- d. Award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;
- e. Grant declaratory relief sought herein;
- f. Award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;
- g. Award pre- and post-judgment interest at the maximum legal rate; and
- h. Grant all such other relief as is just and proper.

JURY DEMAND

Plaintiff demands a trial by jury on all claims so triable.

Respectfully submitted,

DATED: August 13, 2020

By: /s/ Jennie Lee Anderson
Jennie Lee Anderson (SBN 203586)
jennie@andrusanderson.com
ANDRUS ANDERSON LLP
155 Montgomery Street, Suite 900
San Francisco, CA 94104
Telephone: (415) 986-1400
Facsimile: (415) 986-1474

Elizabeth A. Fegan (*motion for pro hac vice forthcoming*)
beth@feganscott.com
FEGAN SCOTT LLC
150 S. Wacker Dr., 24th Floor
Chicago, IL 60606
Telephone: (312) 741-1019
Facsimile: (312) 264-0100

Lynn A. Ellenberger (*motion for pro hac vice forthcoming*)
lynn@feganscott.com
FEGAN SCOTT LLC
500 Grant St., Suite 2900
Pittsburgh, PA 15219
Telephone: (412) 346-4104
Facsimile: (412) 785-2400

Greg T. Kinskey (*motion for pro hac vice forthcoming*)
greg@feganscott.com
FEGAN SCOTT LLC
100 Congress Avenue, Suite 2000
Austin, TX 78701
Telephone: (512) 229-0655
Facsimile: (312) 264-0100

J. Barton Goplerud (*motion for pro hac vice forthcoming*)
goplerud@sagwlaw.com
**SHINDLER, ANDERSON,
GOPLERUD & WEESE, P.C.,**
5015 Grand Ridge Drive, Suite 100
West Des Moines, IA 50265
Telephone: (515) 223-4567
Facsimile: (515) 223-8887

Attorneys for Plaintiff