

1 JENNIE LEE ANDERSON (SBN 203586)

2 jennie@andrusanderson.com

3 ANDRUS ANDERSON LLP

4 155 Montgomery Street, Suite 900

5 San Francisco, CA 94104

6 Telephone: (415) 986-1400

7 Facsimile: (415) 986-1474

8 ELIZABETH A. FEGAN (*pro hac vice forthcoming*)

9 beth@feganscott.com

10 FEGAN SCOTT LLC

11 150 S. Wacker Dr., 24th Floor

12 Telephone: (312) 741-1019

13 Facsimile: (312) 264-0100

14 *Attorneys for Plaintiffs (Additional Counsel Listed on Signature Page)*

15 **UNITED STATES DISTRICT COURT**

16 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**

17 JOSEPH MARTINEZ IV and DANIEL PETRO,
18 individually and on behalf of all others similarly
19 situated,

20 Plaintiffs,

21 v.

22 ZYNGA INC.,

23 Defendant.

Case No. 3:20-cv-02612

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

I. INTRODUCTION 1

II. PARTIES 2

III. JURISDICTION AND VENUE 3

IV. INTRADISTRICT ASSIGNMENT..... 3

V. FACTS 4

 A. Zynga provides “free” games in exchange for its users’ PII. 4

 B. Zynga collected PII from minors. 5

 C. With only non-existent or outdated encryption systems in place to protect customer PII, the PII of Plaintiffs and the Class were stolen from Zynga. 6

 D. Zynga has failed to adequately notify and protect its customers since learning of the data breach. 9

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

VI. CLASS ACTION ALLEGATIONS 13

VII. CLAIMS 16

VIII. PRAYER FOR RELIEF..... 37

1 Plaintiffs Joseph Martinez IV and Daniel Petro, individually and on behalf of all other persons
2 similarly situated, by and through their attorneys, for their Complaint against Defendant Zynga, Inc.,
3 allege as follows:

4 **I. INTRODUCTION**

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

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

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

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

21 5. Since the Zynga Data Breach, Zynga’s customers have been exposed to credit and
22 identity theft, “credit stuffing,” phishing scams, and any other fraudulent conduct that a criminal mind
23 can concoct. Plaintiffs have and will incur costs to mitigate the risk for the data breach, such as
24 paying for credit monitoring services, and will have to spend countless hours monitoring their credit
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 reports and credit card statements. Regardless of whether they have yet to incur out-of-pocket losses,
2 Plaintiffs and all Zynga customers whose PII was stolen remain subject to a pervasive, substantial,
3 and imminent risk of identity theft and fraud now and for years to come.

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

7 II. PARTIES

8 7. Plaintiff Joseph Martinez IV is a resident and citizen of the State of Colorado and at all
9 relevant times resided in Castle Rock, Colorado. In or about 2011, Mr. Martinez provided his PII to
10 Zynga in order to create an account to access and play Zynga games, and in doing so, provided his PII
11 to Zynga. Mr. Martinez played *Words with Friends*, *Words with Friends 2*, *Solitaire*, *Draw*
12 *Something*, and *Zynga Poker*, and made in-game purchases in *Words with Friends*, and perhaps
13 others.

14 8. Mr. Martinez's PII was stolen in the Zynga Data Breach. Mr. Martinez did not receive
15 any notice from Zynga regarding the Zynga Data Breach, and only learned about it recently. Mr.
16 Martinez confirmed through the website haveibeenpwned.com that his email was accessed in the
17 Zynga Data Breach.

18 9. Plaintiff Joseph Martinez IV provided his PII to Zynga with the expectation and
19 understanding that Zynga would adequately protect and store the data. If he had known that Zynga's
20 data security measures and protections were insufficient to protect his PII, he would not have created
21 a Zynga user account and downloaded and played Zynga games, and would not have made in-game
22 purchases. As a result, Plaintiff has been damaged.

23 10. Plaintiff Daniel Pietro is a resident and citizen of the State of Iowa and at all relevant
24 times resided in Des Moines, Iowa. In or about 2007, Plaintiff provided PII to Zynga in order to create
25 an account to access and play Zynga games. Mr. Pietro played the Zynga games *FarmVille*, *Words*
26 *with Friends*, *Zynga Poker*, and *Mafia Wars*, and made in-game purchases in *Mafia Wars* and
27 *FarmVille*.

1 11. Mr. Petro's PII was stolen in the Zynga Data Breach. Mr. Petro did not receive any
2 notice from Zynga regarding the Zynga Data Breach, and only learned about it recently. Mr. Petro
3 confirmed through the website haveibeenpwned.com that his email was accessed in the Zynga Data
4 Breach.

5 12. Plaintiff Daniel Petro provided his PII to Zynga with the expectation and understanding
6 that Zynga would adequately protect and store the data. If he had known that Zynga's data security
7 measures and protections were insufficient to protect his PII, he would not have created a Zynga user
8 account and downloaded and played Zynga games, and would not have made in-game purchases. As
9 a result, Mr. Petro has been damaged.

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

12 **III. JURISDICTION AND VENUE**

13 14. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of
14 2005, 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of \$5,000,000 exclusive of
15 interest and costs, there are more than 100 putative Class members, and Zynga is a citizen of a state
16 different from that of at least one Class member.

17 15. This Court has personal jurisdiction over Zynga because Zynga is headquartered in this
18 state and regularly transacts business in this state.

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

22 **IV. INTRADISTRICT ASSIGNMENT**

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

26 //

27 //

28 //

V. FACTS

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

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

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

20. Zynga’s games are accessible on mobile platforms, Facebook, and other social networks, as well as Zynga.com. Zynga offers a mix of paid and “free” games, which are available for download. Zynga’s “free” games are supported by in-game advertisements, in-game purchases, and its collection of users’ PII.

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

22. To play a Zynga game, the consumer must create a Zynga user account by providing their first name, last name, email address, and gender, and must create a password for the account. At

² <https://www.zynga.com/#> (last visited 4/6/20).

³ <https://www.crunchbase.com/organization/zynga#section-overview> (last visited 4/6/20).

⁴ “Average monthly active users (MAU) of Zynga games from 4th quarter 2012 to 4th quarter 2019,” found at <https://www.statista.com/statistics/273569/monthly-active-users-of-zynga-games/> (last visited 4/6/20).

⁵ “Words With Friends trumps Pokemon GO as most popular US mobile game in March 2017 with 13 million users” (5/4/17) found at <https://www.pocketgamer.biz/news/65662/words-with-friends-13-million-users-march-2017/> (last visited 4/6/20).

⁶ “FarmVille Maker Zynga Is Booming Again” (1/3/2020), found at <https://www.bloomberg.com/news/articles/2020-01-03/zynga-is-booming-again-after-wilderness-years-at-farmville-maker> (last visited 4/6/20).

1 all relevant times and based upon information and belief, Zynga did not collect information regarding
2 a user's age or date of birth, and thus, minors were able to and did create Zynga accounts.

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

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

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

12 25. One study estimates that 8% of all mobile gamers are ages 13-17,⁷ and based upon
13 information and belief, Zynga is aware that a substantial portion of its user base has been and
14 continues to be minors.

15 26. In fact, Zynga acknowledged in Securities and Exchange Commission filings that it is
16 subject to laws and regulations concerning the protection of minors, and that the "increased attention
17 being given to the collection of data from minors" has required it to devote significant operational
18 resources and incur significant expenses.⁸

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

24 ⁷ "The Mobile Gaming Industry: Statistics, Revenue, Demographics, More [Infographic]," (2/6/19),
25 found at <https://mediakix.com/blog/mobile-gaming-industry-statistics-market-revenue/> (last visited
4/6/20).

26 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 4/6/20).

27 ⁹ "Facebook knowingly duped game-playing kids and their parents out of money," (1/24/19), found at
28 <https://www.revealnews.org/article/facebook-knowingly-duped-game-playing-kids-and-their-parents-out-of-money/> (last visited 4/8/20).

1 28. Facebook encouraged game developers such as Zynga to let children spend money
2 without their parents' permission, which Facebook called "friendly fraud," in an effort to maximize
3 revenues.¹⁰ The children oftentimes did not know that they were spending money because while these
4 games are free to download, they are packed with opportunities to spend actual money to advance
5 further. These cash payments are designed to look like items within the game, making it difficult for
6 a child to recognize that they are spending money.¹¹

7 29. Children's PII is particularly attractive to identity thieves. Children's credit reports are
8 clean, and minors do not check their credit reports or review monthly bills, which means thieves may
9 not get caught for years or even decades. And a child's credit cannot be frozen because most children
10 do not have credit information or reports.¹²

11 30. For these reasons and others, "[c]hild identity theft is a growing problem in the United
12 States."¹³

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

15 31. On September 29, 2019, *The Hacker News* reported that a serial hacker from Pakistan
16 called "Gnosticplayers" breached Zynga's *Words with Friends* and improperly accessed a "massive
17 database" of more than 218 million users. The hacker reported that the breach affected all Android
18 and iOS game players who had installed and signed up for the *Words with Friends* game on or before
19 September 2, 2019. The information stolen included names, email addresses, login IDs, passwords,
20 password reset tokens, phone numbers, Facebook IDs and Zynga account IDs.¹⁴

21 _____
¹⁰ *Id.*

22 ¹¹ "Documents Show Facebook Knowingly Took Money from Unwitting Children," (1/25/19), found
23 at <https://www.popularmechanics.com/technology/apps/a26041842/documents-show-facebook-knowingly-took-money-from-unwitting-children/> (last visited 4/8/20)>

24 ¹² "Identity Theft Poses Extra Troubles for Children," (4/17/15), found at
25 <https://www.nytimes.com/2015/04/18/your-money/a-childs-vulnerability-to-identity-theft.html?searchResultPosition=1> (last visited 4/8/20).

26 ¹³ "Never Too Young to Have Your Identity Stolen," (7/21/07), found at
27 <https://www.nytimes.com/2007/07/21/business/21idtheft.html?searchResultPosition=2> (last visited
4/8/20).

28 ¹⁴ "Exclusive — Hacker Steals Over 218 Million Zynga 'Words with Friends' Gamers Data"
(9/29/19), found at <https://thehackernews.com/2019/09/zynga-game-hacking.html> (last visited
4/6/20).

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

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

10 34. That millions of passwords were maintained in plain text and others in SHA-1 confirms
11 that Zynga had inadequate security measures in place to protect and store its users’ PII.

12 35. Industry watchers have speculated that it is possible that all of Zynga’s accounts dating
13 back to the launch of each game accessed by the hacker have been compromised.¹⁸

14 36. Zynga knew it was vulnerable to such attacks. As early as 2012, in a Securities and
15 Exchange Commission (“SEC”) filing, Zynga reported prior hacking attacks and acknowledged that it
16 “will continue to experience hacking attacks.” Zynga recognized that it was “a particularly attractive
17 target for hackers,” because of its prominence in the social gaming industry. It reported that it had
18 previously been the subject of “civil claims alleging liability for the breach of data privacy.”¹⁹

19 37. The Hacker Gnosticplayers, responsible for the recent Zynga attack, is undoubtedly a
20 thief. Gnosticplayers “is a known quantity in the digital criminal underground, having been observed
21

22 _____
23 ¹⁵ “Password Breach of Game Developer Zynga Compromises 170 Million Accounts” (12/30/19),
24 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/)
25 [compromises-170-million-accounts/](https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/) (last visited 4/6/20).

26 ¹⁶ “The SHA1 hash function is now completely unsafe,” (2/23/17), found at
27 [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 4/6/20).

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

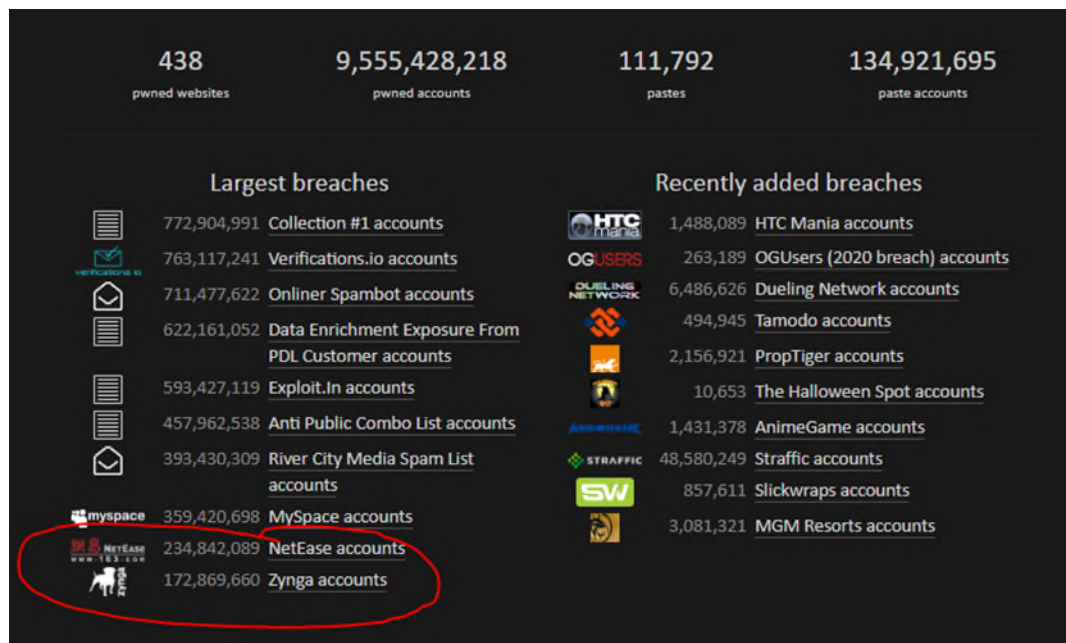
¹⁸ *Id.*

¹⁹ Zynga Inc., Form 10-K, Fiscal Year Ended December 31, 2012, found at
<https://www.sec.gov/Archives/edgar/data/1439404/000119312513072858/d489727d10k.htm> (last
visited 4/8/20).

1 selling hundreds of millions of breached accounts on the dark web since early 2019.”²⁰

2 Gnosticplayers had also claimed responsibility for two previous hacking incidents of other websites,
3 one in February, 2019 and the second in March, 2019, where the hacker put information for millions
4 of accounts for sale on the dark web.²¹ “It should be assumed that all of these stolen passwords [from
5 the Zynga Data Breach] will be available in the wild at some point, if they are not already.”²²

6 38. All told, the Zynga Data Breach exposed the information of over 170 million of Zynga’s
7 customers. According to the website haveibeenpwned.com, the Zynga Data Breach is the tenth
8 largest of all time.²³



21 ²⁰ “Password Breach of Game Developer Zynga Compromises 170 Million Accounts,” *supra*.

22 ²¹ <https://thehackernews.com/2019/09/zynga-game-hacking.html>, *supra*. See also “Times when
23 ‘Gnosticplayers’ hacker made headlines for selling troves of stolen data on dark web,” (9/30/19),
24 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
latest victim of ‘Gnosticplayers’ hacker”) (last visited 4/8/20).

25 ²² “Password Breach of Game Developer Zynga Compromises 170 Million Accounts,” *supra*.

26 ²³ <https://haveibeenpwned.com/> (last visited 4/6/20). The website haveibeenpwned.com is a free
27 online resource for an individual to assess if they may have been put at risk due to an online account
28 having been compromised or “pwned” in a data breach. See also
<https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/>, *supra* (“The amount of account records compromised would
make this the 10th largest data breach of all time”).

1
2 **D. Zynga has failed to adequately notify and protect its customers since learning of**
3 **the data breach.**

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

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

12 Player Security Announcement

13 Sep 12, 2019

 PDF Version

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

17 While the investigation is ongoing, we do not believe any financial information was accessed. However, we have identified account login information for
18 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'
19 accounts from invalid logins. We plan to further notify players as the investigation proceeds.

20 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
21 community. Additional information is available on our [Player Support](#) page.

22 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](#)
23 [2019 Quarterly Earnings Letter](#) on July 31, 2019.

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

²⁴ <https://investor.zynga.com/news-releases/news-release-details/player-security-announcement> (last visited 4/7/20).

²⁵ *Id.*

²⁶ *Id.*

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

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

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

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

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

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

25 _____
26 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/)
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, CEO of CybSafe, a cyber security
28 awareness platform and cloud data analytics platform).

²⁸ *Id.*

²⁹ “Hacker Lexicon: What Is Credential Stuffing?” (2/17/19) found at
<https://www.wired.com/story/what-is-credential-stuffing/> (last visited 4/6/20).

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

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

8 50. In addition, because some customers have their games connected to their Facebook
9 accounts, hackers can gain access to far more information to create a forged identity. “Logging in
10 with this stolen information (including the 7 million *Draw Something* passwords left in clear text with
11 this breach) makes it impossible to determine if the actual account holder is the one logging in.”³²

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

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

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

22 In addition to the losses that result when identity thieves fraudulently open
23 accounts . . . individual victims often suffer indirect financial costs,
24 including the costs incurred in both civil litigation initiated by creditors

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

26 ³¹ <https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/>, *supra*.

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

28 ³³ “Facts + Statistics: Identity theft and cybercrime,” found at <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (last visited 2/8/20).

1 and in overcoming the many obstacles they face in obtaining or retaining
2 credit. Victims of non-financial identity theft, for example, health-related
or criminal record fraud, face other types of harm and frustration.

3 In addition to out-of-pocket expenses that can reach thousands of dollars
4 for the victims of new account identity theft, and the emotional toll
5 identity theft can take, some victims have to spend what can be a
6 considerable amount of time to repair the damage caused by the identity
7 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

8 53. The indirect costs of identity theft take victims away from their everyday lives. They
9 spend less time on hobbies and vacations, and are forced to take time off of work and spend time
10 away from their family. In 2016, more than 25% of victims had to borrow money from family and
11 friends.³⁵

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

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

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

21 57. The physical and emotional responses caused by identity theft can exist for years at a
22

23 ³⁴ “The President’s Identity Theft Task Force, Combating Identity Theft, A Strategic Plan” (April
24 2007), p.11, found at [https://www.ftc.gov/sites/default/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) (last visited 4/8/20).

25 ³⁵ “Identity Theft: The Aftermath 2017,” p.7, found at [https://www.idtheftcenter.org/images/page-
docs/Aftermath_2017.pdf](https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf) (last visited 4/9/20).

26 ³⁶ *Id.*

27 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](https://www.nbcnews.com/business/consumer/not-just-financial-toll-some-victims-identity-theft-consider-suicide-n817966) (last visited 4/8/20).

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

1 time. According to the U.S. Government Accountability Office, which conducted a study regarding
2 data breaches, use of stolen data can occur years into the future:

3 [L]aw enforcement officials told us that in some cases, stolen data may be
4 held for up to a year or more before being used to commit identity theft.
5 Further, once stolen data have been sold or posted on the Web, fraudulent
6 use of that information may continue for years. As a result, studies that
7 attempt to measure the harm resulting from data breaches cannot
8 necessarily rule out all future harm.³⁹

9 58. Plaintiffs and the Class had their PII stolen in the Zynga Data Breach, causing Plaintiffs
10 and the Class to suffer injuries and damages, including but not limited to the improper disclosure of
11 PII, the loss of value of the PII, disclosure and dissemination of the PII, the actual and imminent threat
12 of identity theft and other fraud, the loss of privacy, and out-of-pocket expense and time devoted to
13 mitigating the effects of the data breach.

13 VI. CLASS ACTION ALLEGATIONS

14 59. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, Plaintiffs seek
15 certification of the following Nationwide Class: “All persons residing in the United States whose PII
16 was compromised in the Zynga Inc. data breach that occurred in or around September, 2019.”

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

23 61. **Commonality and Predominance: Federal Rules of Civil Procedure 23(a)(2) and**
24 **23(b)(3).** This action involves common questions of law and fact, which predominate over any
25 questions affecting individual Class members, including:
26

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 4/8/20).

- 1 a. Whether Defendant knew or should have known that its computer and data
- 2 systems were vulnerable to attack;
- 3 b. Whether Defendant failed to take adequate and reasonable measures to ensure its
- 4 computer and data systems were protected;
- 5 c. Whether Defendant failed to take available steps to prevent and stop the breach
- 6 from happening;
- 7 d. Whether Defendant failed to disclose the material facts that it did not have
- 8 adequate security practices and systems to safeguard its customers' PII;
- 9 e. Whether Defendant failed to provide timely and adequate notice of the data
- 10 breach;
- 11 f. Whether Defendant owed a duty to Plaintiffs and Class members to protect their
- 12 PII and to provide timely and accurate notice of the data breach to Plaintiffs and
- 13 Class members;
- 14 g. Whether Defendant breached its duties to protect the PII of Plaintiffs and Class
- 15 members by failing to provide adequate security and by failing to provide timely
- 16 and accurate notice to Plaintiffs and Class members of the data breach;
- 17 h. Whether Defendant's actions or inactions resulted in or was the proximate cause
- 18 of the breach of its systems, resulting in the unauthorized access and/or theft of
- 19 Plaintiffs' and Class members' PII;
- 20 i. Whether Defendant's conduct violated state consumer protection laws;
- 21 j. Whether Defendant's conduct renders it liable for negligence, negligence per se,
- 22 breach of contract, breach of implied contract, unjust enrichment, and breach of
- 23 confidence;
- 24 k. Whether, as a result of Defendant's conduct, Plaintiffs and Class members face a
- 25 significant threat of harm and/or have already suffered harm, and, if so, the
- 26 appropriate measure of damages to which they are entitled;
- 27
- 28

1 l. Whether, as a result of Defendant’s conduct, Plaintiffs and Class members are
2 entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the
3 nature of such relief; and

4 m. Whether, as a result of Defendant’s conduct, Plaintiffs and Class members are
5 entitled to damages, punitive damages, costs, and attorneys’ fees.

6 62. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs’ claims are typical of
7 other Class members’ claims because Plaintiffs and Class members were subjected to the same
8 allegedly unlawful conduct and damaged in the same way.

9 63. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are
10 adequate class representatives because their interests do not conflict with the interests of Class
11 members who they seeks to represent, Plaintiffs have retained counsel competent and experienced in
12 complex class action litigation, and Plaintiffs intends to prosecute this action vigorously. The Class
13 members’ interests will be fairly and adequately protected by Plaintiffs and their counsel.

14 64. **Declaratory and Injunctive Relief: Federal Rule of Civil Procedure 23(b)(2).**
15 Defendant has acted and/or refused to act on grounds generally applicable to the Class, making final
16 injunctive relief or corresponding declaratory relief appropriate.

17 65. **Superiority: Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any
18 other available means for the fair and efficient adjudication of this controversy, and no unusual
19 difficulties are likely to be encountered in the management of this class action. The damages or other
20 financial detriment suffered by Plaintiffs and Class members are relatively small compared to the
21 burden and expense that would be required to individually litigate their claims against Defendant, so it
22 would be impracticable for Class members to individually seek redress for Defendant’s wrongful
23 conduct. Even if Class members could afford litigation, the court system could not. Individualized
24 litigation creates a potential for inconsistent or contradictory judgments and increases the delay and
25 expense to all parties and the court system. By contrast, the class action device presents far fewer
26 management difficulties and provides the benefits of single adjudication, economies of scale, and
27 comprehensive supervision by a single court, especially where there are over 172 million Zynga users
28 affected.

VII. CLAIMS

**COUNT I
NEGLIGENCE**

ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS

1
2
3
4 66. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

5 67. Defendant owed a duty to Plaintiffs and Class members to exercise reasonable care in
6 obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from
7 being compromised, lost, stolen, accessed, and misused by unauthorized persons.

8 68. This duty included, among other things:

- 9 a. designing, maintaining, and testing its security systems to ensure that Plaintiffs'
10 and Class members' PII in its possession was adequately secured and protected;
11 b. implementing processes that would detect a breach of its security system in a
12 timely manner;
13 c. timely acting upon warnings and alerts, including those generated by its own
14 security systems, regarding intrusions to its networks;
15 d. maintaining data security measures consistent with current technology and
16 industry standards; and
17 e. timely notifying customers that their PII had been compromised, lost, stolen,
18 accessed, or misused.

19 69. Defendant's duty to use reasonable care arose from several sources. Defendant had a
20 common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and
21 Class members were the foreseeable and probable victims of any inadequate security practices.

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

26 71. Defendant's duty to Plaintiffs and Class members also arose because of a special
27 relationship that existed between Defendant and Plaintiffs and Class members. That special
28 relationship arose because Plaintiffs and the Class member entrusted Defendant with their PII as part

1 of the creation of user accounts necessary to access Zynga’s online and mobile gaming applications.
2 Defendant could have ensured that its security systems and data protection measures were sufficient
3 to minimize or prevent the data breach.

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

11 73. Defendant breached the duties it owed to Plaintiffs and Class members described above
12 and thus was negligent. Defendant breached these duties by, among other things, failing to: (a)
13 exercise reasonable care and implement adequate security systems, protocols and practices sufficient
14 to protect the PII of Plaintiffs and Class members; (b) detect the breach while it was ongoing; (c)
15 maintain security systems consistent with current technology and industry standards; and (d) timely
16 disclose that Plaintiffs’ and Class members’ PII in Defendant’s possession had been or was
17 reasonably believed to have been, stolen or compromised.

18 74. Timely notification of the data breach was required, appropriate, and necessary so that,
19 among other things, Plaintiffs and Class members could take appropriate measures to freeze or lock
20 their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or
21 change usernames and passwords on compromised accounts, monitor their account information and
22 credit reports for fraudulent activity, contact their banks or other financial institutions that issue their
23 credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate
24 the damages caused by Defendant’s misconduct.

25 75. But for Defendant’s wrongful and negligent breach of its duties owed to Plaintiffs and
26 Class members, their PII would not have been compromised.

27 76. As a direct and proximate result of Defendant’s negligence, Plaintiffs and Class
28 members have been injured as described herein, and are entitled to damages, including compensatory,

1 punitive, and nominal damages, in an amount to be proven at trial.

2 77. Plaintiffs' and Class members' injuries include:

- 3 a. theft of their PII;
- 4 b. costs associated with the detection and prevention of identity theft and
5 unauthorized use of their financial accounts;
- 6 c. costs associated with purchasing credit monitoring and identity theft protection
7 services;
- 8 d. unauthorized charges and loss of use of and access to their financial account
9 funds and costs associated with inability to obtain money from their accounts or
10 being limited in the amount of money they were permitted to obtain from their
11 accounts, including missed payments on bills and loans, late charges and fees,
12 and adverse effects on their credit;
- 13 e. lowered credit scores resulting from credit inquiries following fraudulent
14 activities;
- 15 f. costs associated with time spent and the loss of productivity from taking time to
16 address and attempt to ameliorate, mitigate, and deal with the actual and future
17 consequences of the data breach — including finding fraudulent charges,
18 cancelling and reissuing cards, enrolling in credit monitoring and identity theft
19 protection services, freezing and unfreezing accounts, and imposing withdrawal
20 and purchase limits on compromised accounts;
- 21 g. the physical and emotional injuries caused by being victimized by a data breach;
- 22 h. the imminent and certainly impending injury flowing from potential fraud and
23 identify theft posed by their PII being placed in the hands of criminals; and
- 24 i. continued risk of exposure to hackers and thieves of their PII, which remains in
25 Defendant's possession and is subject to further breaches so long as Defendant
26 fails to undertake appropriate and adequate measures to protect Plaintiffs and
27 Class members.

28 //

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

COUNT II
NEGLIGENCE PER SE
ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS

78. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

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

80. Defendant violated Section 5 of the FTCA (and similar state statutes) by failing to use reasonable measures to protect Plaintiffs’ and Class members’ PII, failing to use current and generally accepted technology, and not complying with industry standards. Defendant’s conduct was particularly unreasonable given the size of its customer database, the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach.

81. Defendant’s violation of Section 5 of the FTCA (and similar state statutes) constitutes negligence per se.

82. Plaintiffs and Class members are not seeking to hold Defendant liable under the FTCA, itself. Instead, that section forms the basis of Defendants’ duty to Plaintiffs and Class members.

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

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

85. As a direct and proximate result of Defendant’s negligence, Plaintiffs and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

**COUNT III
BREACH OF CONTRACT
ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS**

86. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

87. Zynga’s Privacy Policy (the “Privacy Policy”) is an agreement between Zynga and persons who provide their PII to Zynga, including Plaintiffs and Class members.

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

89. The Privacy Policy, as it was in effect at the time of the Zynga Data Breach, stated that it applies to persons who use Zynga’s services, meaning games, products, services, content, Zynga.com, and/or domain or website operated by Zynga, and it details how Zynga will both protect and use the PII provided by users of Zynga’s services.

90. Plaintiffs and Class members on the one hand and Zynga on the other formed a contract when Plaintiffs and Class members provided PII to Zynga subject to the Privacy Policy and used Zynga’s services.

91. Plaintiffs and Class members fully performed their obligations under the contract with Zynga.

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

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

**COUNT IV
BREACH OF IMPLIED CONTRACT
ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS**

94. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

1 95. This claim is an alternative to Plaintiffs' and the Nationwide Class' breach of contract
2 claim.

3 96. Plaintiffs and Class members alternatively entered into an implied contract with Zynga
4 when they obtained services from Zynga, or otherwise provided PII to Zynga.

5 97. As part of these transactions, Zynga agreed to safeguard and protect the PII of Plaintiffs
6 and Class members.

7 98. Plaintiffs and Class members entered into implied contracts with the reasonable
8 expectation that Zynga's data security practices and policies were reasonable and consistent with
9 industry standards. Under the implied contracts, Plaintiffs and Class members believed that
10 Defendant would use part of the monies paid to Zynga or monies it derived from advertising to
11 provide reasonable and adequate data security to protect Plaintiffs' and Class members' PII.

12 99. Plaintiffs and Class members would not have provided and entrusted their PII to Zynga
13 and/or would have paid less in the absence of the implied contract or implied terms between them and
14 Zynga. The safeguarding of the PII of Plaintiffs and Class members was critical to realize the intent
15 of the parties' bargain.

16 100. Plaintiffs and Class members fully performed their obligations under the implied
17 contracts with Zynga.

18 101. Zynga breached its implied contracts with Plaintiffs and Class members by failing to
19 protect their PII. Specifically, Defendant (1) failed to use reasonable measures to protect that
20 information; and (2) disclosed that information to unauthorized third parties, in violation of the
21 implied agreement.

22 102. As a direct and proximate result of these breaches of implied contract, Plaintiffs and
23 Class members sustained actual losses and damages as described in detail above, including but not
24 limited to being denied the benefit of the bargain pursuant to which they provided their PII to Zynga.

25 **COUNT V**
26 **UNJUST ENRICHMENT**
27 **ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS**

28 103. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

1 104. This claim is an alternative to Plaintiffs' breach of contract and breach of implied
2 contract claims.

3 105. Plaintiffs and Class members have an equitable and legal interest in their PII that was
4 conferred upon, collected by, and maintained by Defendant and that was ultimately stolen in the data
5 breach.

6 106. Defendant benefited from the collection of Plaintiffs and the Class' PII, and its ability to
7 retain, use, and profit from that information. Defendant understood the benefit of collecting and
8 possessing this information.

9 107. Defendant also understood that Plaintiffs' and the Class' PII was private and
10 confidential and its value depended upon Defendant maintaining the privacy and confidentiality of
11 that PII.

12 108. But for Defendant's willingness and commitment to maintain its privacy and
13 confidentiality, Plaintiffs and Class members would not have provided their PII to the Defendant.

14 109. Defendant continues to benefit and profit from its retention and use of the PII while its
15 value to Plaintiffs and Class members has been diminished.

16 110. Defendant benefitted by Plaintiffs and Class members' purchases of mobile gaming
17 applications or in-game items, or using Defendant's free gaming applications where paid advertising
18 was displayed, and this benefit was more than those services were worth to Plaintiffs and Class
19 members had been aware that Defendant would fail to protect their PII.

20 111. Zynga also benefitted through its unjust conduct by retaining money that it should have
21 used to provide reasonable and adequate data security to protect Plaintiffs' and Class members' PII.

22 112. It is inequitable for Defendant to retain these benefits.

23 113. As a result of Defendant's wrongful conduct including, among other conduct, its
24 knowing failure to employ adequate data security measures, its continued maintenance and use
25 Plaintiffs' and Class members' PII without having adequate data security measures, and its other
26 conduct facilitating the theft of that PII, Defendant has been unjustly enriched at the expense of, and
27 to the detriment of, Plaintiffs and Class members.
28

1 114. Defendant's unjust enrichment is traceable to, and resulted directly and proximately
2 from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class members'
3 PII, while at the same time failing to maintain that information secure from intrusion and theft by
4 hackers and thieves.

5 115. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to
6 be permitted to retain the benefits it received, and is still receiving, without justification, from
7 Plaintiffs and Class members in an unfair and unconscionable manner. Defendant's retention of such
8 benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

9 116. The benefits conferred upon, received, and enjoyed by Defendant were not conferred
10 officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain these
11 benefits.

12 117. Plaintiffs and Class members have no adequate remedy at law.

13 118. Defendant is therefore liable to Plaintiffs and Class members for restitution or
14 disgorgement in the amount of the benefit conferred on Defendant as a result of its wrongful conduct,
15 including specifically: the value to Defendant of the PII that was stolen in the Zynga Data Breach; the
16 profits Defendant is receiving from the use of that information; the amount that Zynga overcharged
17 Plaintiffs and Class members for use of its online and mobile gaming application services through in-
18 app purchases; and the amounts that Zynga should have spent to provide reasonable and adequate data
19 security to protect Plaintiffs' and Class members' PII.

20 **COUNT VI**
21 **BREACH OF CONFIDENCE**
22 **ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS**

23 119. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

24 120. At all times, Defendant was aware of the confidential and sensitive nature of Plaintiffs'
25 and Class members' PII.

26 121. As alleged herein and above, Zynga's relationship with Plaintiffs and Class members was
27 governed by terms of the Privacy Policy and/or the implied expectation that Plaintiffs' and Class
28

1 members' PII would be collected, stored, and protected in confidence, and would not be disclosed to
2 the public or any unauthorized third parties.

3 122. Plaintiffs' and Class members provided their PII to Zynga with the explicit and implicit
4 understandings that Defendant would protect and not permit the PII to be disseminated to the public or
5 any unauthorized parties.

6 123. Plaintiffs and Class members also provided their respective PII to Zynga with the explicit
7 and implicit understandings that Defendant would take precautions to protect the PII from unauthorized
8 disclosure, such as following basic principles of encryption and information security practices.

9 124. Zynga voluntarily received in confidence Plaintiffs' and Class members' PII with the
10 understanding that PII would not be disclosed or disseminated to the public or any unauthorized third
11 parties.

12 125. Due to Zynga's failure to prevent, detect, avoid the data breach from occurring by
13 following best systems and security practices to secure Plaintiffs' and Class members' PII, Plaintiffs'
14 and Class members' PII was disclosed and misappropriated to unauthorized third parties and the public
15 beyond Plaintiffs' and Class members' confidence, and without their express permission.

16 126. But for Defendant's disclosure of Plaintiffs' and Class members' PII in violation of the
17 parties' understanding of confidence, their PII would not have been compromised, stolen, viewed,
18 accessed, and used by unauthorized third parties. The Zynga Data Breach was the direct and legal cause
19 of the theft of Plaintiffs' and Class members' PII, as well as the resulting damages.

20 127. The injury and harm Plaintiffs and Class members suffered was the reasonably
21 foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class members' PII. Zynga
22 knew its computer systems for accepting, securing, and storing Plaintiffs' and Class members' PII had
23 serious security vulnerabilities where Zynga failed to observe even basic information security practices
24 or correct known security vulnerabilities.

25 128. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and
26 Class members have been injured as described herein, and are entitled to damages, including
27 compensatory, punitive, and nominal damages, in an amount to be proven at trial.

28 //

COUNT VII
VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW
CAL. BUS. & PROF. CODE, §§ 17200, ET SEQ.
ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS

129. Plaintiffs reallege and incorporate the foregoing allegations as if fully set forth herein.

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

131. Defendant is a “person” as defined by Cal. Bus. & Prof. Code §17201.

132. Defendant’s unlawful, unfair, and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security measures to protect Plaintiffs’ and Class members’ PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the data breach.
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the data breach. This conduct was unfair when weighed against the harm to Plaintiffs and Class members, whose PII has been compromised;
- c. Failing to implement and maintain reasonable security measures, which was contrary to legislatively declared public policy that seeks to protect consumers’ data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTCA, 15 U.S.C. § 45, and California’s Consumer Records Act, Cal. Civ. Code § 1798.81.5;
- d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs’ and Class members’ PII, including duties imposed by the FTCA, 15 U.S.C. § 45 and California’s Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., which was a direct and proximate cause of the data breach;

- 1 e. Failing to implement and maintain reasonable security measures, which led to
2 substantial injuries, as described above, that are not outweighed by any
3 countervailing benefits to consumers or competition. Moreover, because
4 consumers could not know of Defendant's inadequate security, consumers could
5 not have reasonably avoided the harms that Defendant caused;
- 6 f. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82,
7 by failing to disclose a data security breach and failing to notify or timely notify
8 Plaintiffs and Class members that their PII had been accessed and stolen;
- 9 g. Misrepresenting in its Privacy Policy and elsewhere that it would protect the
10 privacy and confidentiality of Plaintiffs' and Class members' PII, including by
11 implementing and maintaining reasonable security measures;
- 12 h. Omitting, suppressing, and concealing the material fact that it did not reasonably
13 or adequately secure Plaintiffs' and Class members' PII;
- 14 i. Omitting, suppressing, and concealing the material fact that it did not comply
15 with common law and statutory duties pertaining to the security and privacy of
16 Plaintiffs' and Class members' PII, including duties imposed by the FTCA, 15
17 U.S.C. § 45 and California's Customer Records Act, Cal. Civ. Code §§ 1798.80,
18 et seq.; and
- 19 j. Failing to notify Plaintiffs and Class members that their PII had been accessed
20 and stolen.

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

26 134. Defendant's representations and omissions were material because they were likely to
27 deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect
28 the confidentiality of consumers' PII.

1 135. Defendant had exclusive knowledge of material facts not known to Plaintiffs and Class
2 members and Defendant made partial representations but also suppressed some material facts.

3 136. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts
4 and practices, Plaintiffs and Class members were injured and lost money or property: the money
5 received by Zynga for its services; the loss of the benefit of their bargain with and overcharges by
6 Zynga as they would not have paid Zynga for services or would have paid less for such services but
7 for the violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and
8 identity protection services; time and expenses related to monitoring their financial accounts for
9 fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity
10 theft.

11 137. Defendant acted intentionally, knowingly, and maliciously to violate California's UCL,
12 and recklessly disregarded Plaintiffs' and Class members' rights and interests. As disclosed in SEC
13 filings, Defendant knew that its security and privacy protections were vulnerable to attack, and
14 Defendant knew that its security measures were inadequate in the face of such attack.

15 138. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by
16 law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent
17 business practices or use of their PII; declaratory relief; injunctive relief; and other appropriate
18 equitable relief.

19 **COUNT VIII**
20 **VIOLATIONS OF THE CALIFORNIA FALSE ADVERTISING LAW**
21 **CAL. BUS. & PROF. CODE § 17500, ET SEQ.**
22 **ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS**

23 139. Plaintiffs incorporate by reference all paragraphs as though fully set forth herein.

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

27 141. Section 17500 of the Cal. Bus. & Prof. Code states: "It is unlawful for any . . .
28 corporation . . . with intent directly or indirectly . . . to perform services, professional or otherwise, or
anything of any nature whatsoever or to induce the public to enter into any obligation relating thereto,

1 to make or disseminate or cause to be made or disseminated before the public in this state, or to make
 2 or disseminate or cause to be made or disseminated from this state before the public in any state, in
 3 any newspaper or other publication, or any advertising device, . . . or in any other manner or means
 4 whatever, including over the Internet, any statement, concerning that real or personal property or
 5 those services, professional or otherwise, or concerning any circumstance or matter of fact connected
 6 with the proposed performance or disposition thereof, which is untrue or misleading, and which is
 7 known, or which by the exercise of reasonable care should be known, to be untrue or misleading. . . .”

8 142. Defendant caused to be made or disseminated through California and the United States,
 9 through advertising, marketing and other publications, the following statements or omissions that
 10 were untrue or misleading, and which were known, or which by the exercise of reasonable care should
 11 have been known to Defendant, to be untrue and misleading to consumers, including Plaintiffs and the
 12 other Class members:

- 13 a. Failing to disclose that reasonable security measures to protect Plaintiffs’ and
 14 Class members’ PII from unauthorized disclosure, release, data breaches, and
 15 theft, were in place, which was a direct and proximate cause of the data breach.
- 16 b. Failing to disclose foreseeable security and privacy risks, remediate identified
 17 security and privacy risks, and adequately improve security and privacy measures
 18 despite knowing the risk of cybersecurity incidents, which was a direct and
 19 proximate cause of the data breach. This conduct was unfair when weighed
 20 against the harm to Plaintiffs and Class members, whose PII has been
 21 compromised;
- 22 c. Failing to disclose non-compliance with reasonable security measures, which was
 23 contrary to legislatively declared public policy that seeks to protect consumers’
 24 data and ensure that entities that are trusted with it use appropriate security
 25 measures. These policies are reflected in laws, including the FTCA, 15 U.S.C. §
 26 45, and California’s Consumer Records Act, Cal. Civ. Code § 1798.81.5;
- 27 d. Failing to disclose non-compliance with common law and statutory duties
 28 pertaining to the security and privacy of Plaintiffs’ and Class members’ PII,

1 including duties imposed by the FTCA, 15 U.S.C. § 45 and California's
2 Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., which was a direct
3 and proximate cause of the data breach;

- 4 e. Failing to disclose non-compliance with reasonable security measures, which led
5 to substantial injuries, as described above, that are not outweighed by any
6 countervailing benefits to consumers or competition. Moreover, because
7 consumers could not know of Defendant's inadequate security, consumers could
8 not have reasonably avoided the harms that Defendant caused;
- 9 f. Failing to disclose a data security breach in violation of Cal. Civ. Code §
10 1798.82, and failing to notify or timely notify Plaintiffs and Class members that
11 their PII had been accessed and stolen;
- 12 g. Misrepresenting in its Privacy Policy and elsewhere that it would protect the
13 privacy and confidentiality of Plaintiffs' and Class members' PII, including by
14 implementing and maintaining reasonable security measures;
- 15 h. Omitting, suppressing, and concealing the material fact that it did not reasonably
16 or adequately secure Plaintiffs' and Class members' PII; and
- 17 i. Omitting, suppressing, and concealing the material fact that it did not comply
18 with common law and statutory duties pertaining to the security and privacy of
19 Plaintiffs' and Class members' PII, including duties imposed by the FTCA, 15
20 U.S.C. § 45 and California's Customer Records Act, Cal. Civ. Code §§ 1798.80,
21 et seq..

22 143. Defendant violated § 17500 because the misrepresentations and omissions identified
23 above induced Plaintiff and the Class to provide their PII to Defendant, and were therefore material
24 and likely to deceive a reasonable consumer.

25 144. Plaintiffs and Class members have suffered an injury in fact, including the loss of
26 money or property, as a result of Defendant's unlawful, untrue, misleading and deceptive advertising
27 and practices.

1 145. Defendant's representations and omissions were material because they were likely to
2 deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect
3 the confidentiality of consumers' PII.

4 146. Defendant had exclusive knowledge of material facts not known to Plaintiffs and Class
5 members and Defendant made partial representations but also suppressed some material facts.

6 147. As a direct and proximate result of Defendant's unlawful, untrue, misleading and
7 deceptive advertising and practices, Plaintiffs and Class members were injured and lost money or
8 property: the money received by Zynga for its services; the loss of the benefit of their bargain with
9 and overcharges by Zynga as they would not have paid Zynga for services or would have paid less for
10 such services but for the violations alleged herein; losses from fraud and identity theft; costs for credit
11 monitoring and identity protection services; time and expenses related to monitoring their financial
12 accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud
13 and identity theft.

14 148. All of the wrongful conduct alleged herein occurred, and continues to occur, in the
15 conduct of Defendant's business.

16 149. Defendant's wrongful conduct is part of a pattern or generalized course of conduct that
17 is still perpetuated and repeated, both in the State of California and nationwide.

18 150. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by
19 law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent
20 business practices or use of their PII; declaratory relief;; injunctive relief; and other appropriate
21 equitable relief.

22 **COUNT IX**
23 **VIOLATIONS OF THE CALIFORNIA CONSUMERS LEGAL REMEDIES ACT**
24 **CAL. CIV. CODE § 1750, ET SEQ.**
25 **ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS**

26 151. Plaintiffs incorporate by reference all other paragraphs of this Complaint as if fully set
27 forth herein.
28

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

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

11 154. Defendant misrepresented the nature of their products and services in violation of the
12 CLRA by engaging in unlawful, unfair, and deceptive acts and practices including:

- 13 a. Failing to disclose its failure to implement and maintain reasonable security
14 measures to protect Plaintiffs’ and Class members’ PII from unauthorized
15 disclosure, release, data breaches, and theft, which was a direct and proximate
16 cause of the data breach.
- 17 b. Failing to identify foreseeable security and privacy risks, remediate identified
18 security and privacy risks, and adequately improve security and privacy measures
19 despite knowing the risk of cybersecurity incidents, which was a direct and
20 proximate cause of the data breach. This conduct was unfair when weighed
21 against the harm to Plaintiffs and Class members, whose PII has been
22 compromised;
- 23 c. Failing to disclose its failure to implement and maintain reasonable security
24 measures, which was contrary to legislatively declared public policy that seeks to
25 protect consumers’ data and ensure that entities that are trusted with it use
26 appropriate security measures. These policies are reflected in laws, including the
27 FTCA, 15 U.S.C. § 45, and California’s Consumer Records Act, Cal. Civ. Code
28 § 1798.81.5;

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

27 155. As a direct and proximate result of Defendant's unlawful acts and practices, Plaintiffs
28 and Class members were injured and lost money or property: the money received by Zynga for its

1 services; the loss of the benefit of their bargain with and overcharges by Zynga as they would not
 2 have paid Zynga for services or would have paid less for such services but for the violations alleged
 3 herein; losses from fraud and identity theft; costs for credit monitoring and identity protection
 4 services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss
 5 of value of their PII; and an increased, imminent risk of fraud and identity theft.

6 156. Defendant acted intentionally, knowingly, and maliciously to violate California's
 7 CLRA, and recklessly disregarded Plaintiffs' and Class members' rights and interests. As disclosed
 8 in SEC filings, Defendant knew that its security and privacy protections were vulnerable to attack, and
 9 Defendant knew that its security measures were inadequate in the face of such attack.

10 157. Plaintiffs and Class members seek injunctive relief, declaratory relief, reasonable
 11 attorneys' fees and costs, and other appropriate equitable relief.

12 158. On the same day that this Complaint was filed, Plaintiffs have provided Defendant with
 13 notice of its violations of the CLRA and a demand on behalf of themselves and the Class pursuant to
 14 California Civil Code section 1782(a). If after 30 days, Defendant has not agreed satisfied Plaintiffs'
 15 demands in whole and on behalf of all Class members, Plaintiffs will amend this Complaint to seek all
 16 damages stemming from Defendant's unlawful conduct.

17 159. Pursuant to California Civil Code § 1780(d), filed concurrently herewith is the
 18 Declaration of Jennie Lee Anderson showing that this action has been commenced in the proper
 19 forum.

20 **COUNT X**
 21 **ALTERNATIVE COUNT FOR VIOLATIONS OF**
 22 **STATE CONSUMER PROTECTION ACTS**
ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS

23 160. Plaintiffs incorporate by reference all other paragraphs of this Complaint as if fully set
 24 forth herein.

25 161. This claim is an alternative to Plaintiffs' and the Nationwide Class' claims under
 26 California's UCL, FAL and CLRA, and is brought individually, and on behalf of all similarly situated
 27 residents of each of the 50 states for violations of the state consumer protection acts including:
 28

- 1 a. the Alaska Unfair Trade Practices and Consumer Protection Act, Alaska Stat. §
- 2 45.50.471, et seq.;
- 3 b. the Arizona Consumer Fraud Act, Ariz. Rev. Stat. §§ 44-1521, et seq.;
- 4 c. the Arkansas Deceptive Trade Practices Act, Ark. Code § 4-88-101, et seq.;
- 5 d. the California Unfair Competition Law, Bus. & Prof. Code §§ 17200, et seq. and
- 6 17500, et seq.;
- 7 e. the California Consumers Legal Remedies Act, Cal. Civ. Code § 1750, et seq.;
- 8 f. the Colorado Consumer Protection Act, Colo. Rev. Stat. Ann. § 6-1-101, et seq.;
- 9 g. the Connecticut Unfair Trade Practices Act, Conn. Gen Stat. Ann. § 42- 110, et
- 10 seq.;
- 11 h. the Delaware Consumer Fraud Act, 6 Del. Code § 2513, et seq.;
- 12 i. the D.C. Consumer Protection Procedures Act, D.C. Code § 28-3901, et seq.;
- 13 j. the Florida Deceptive And Unfair Trade Practices Act, Fla. Stat. Ann. § 501.201,
- 14 et seq.;
- 15 k. the Georgia Fair Business Practices Act, Ga. Code Ann. § 10-1-390, et seq.;
- 16 l. the Hawaii Unfair Competition Law, Haw. Rev. Stat. § 480-2, et seq.;
- 17 m. the Idaho Consumer Protection Act, Idaho Code. Ann. § 48-601, et seq.;
- 18 n. the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS
- 19 501/1, et seq.;
- 20 o. the Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5-2, et seq.;
- 21 p. the Iowa Consumer Fraud Act, Iowa Code § 714H, et seq.;
- 22 q. the Kansas Consumer Protection Act, Kan. Stat. Ann. § 50-623, et seq.;
- 23 r. the Kentucky Consumer Protection Act, Ky. Rev. Stat. Ann. § 367.110, et seq.;
- 24 s. the Louisiana Unfair Trade Practices And Consumer Protection Law, LSA-R.S.
- 25 51:1401, et seq.;
- 26 t. the Maine Unfair Trade Practices Act, Me. Rev. Stat. Ann. Tit. 5, § 207, et seq.;
- 27 u. the Maryland Consumer Protection Act, Md. Code Ann. Com. Law, § 13-301, et
- 28 seq.;

- 1 v. the Massachusetts Regulation of Business Practices for Consumers Protection
- 2 Act, Mass. Gen Laws Ann. Ch. 93A, et seq.;
- 3 w. the Michigan Consumer Protection Act, Mich. Comp. Laws Ann. § 445.901, et
- 4 seq.;
- 5 x. the Minnesota Prevention of Consumer Fraud Act, Minn. Stat. § 325F, et seq.;
- 6 y. the Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407, et seq.;
- 7 z. the Nebraska Consumer Protection Act, Neb. Rev. St. §§ 59-1601, et seq.;
- 8 aa. the Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. § 41.600, et seq.
- 9 bb. the New Hampshire Regulation of Business Practices For Consumer Protection,
- 10 N.H. Rev. Stat. § 358-A:1, et seq.;
- 11 cc. the New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8, et seq.;
- 12 dd. the New Mexico Unfair Practices Act, N.M. Stat. Ann. § 57-12-1, et seq.;
- 13 ee. the New York Consumer Protection from Deceptive Acts and Practices, N.Y.
- 14 Gen. Bus. Law § 349, et seq.;
- 15 ff. the North Carolina Unfair And Deceptive Trade Practices Act, N.C. Gen Stat. §
- 16 75-1.1, et seq.;
- 17 gg. the North Dakota Consumer Fraud Act, N.D. Cent. Code § 51-15, et seq.;
- 18 hh. the Ohio Consumer Sales Practices Act, Ohio Rev. Code Ann. § 1345.01, et seq.;
- 19 ii. the Oklahoma Consumer Protection Act, Okla. Stat. tit. 15 § 751, et seq.;
- 20 jj. the Oregon Unlawful Trade Practices Act, Or. Rev. Stat. § 646.605, et seq.;
- 21 kk. the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §
- 22 201-1, et seq.;
- 23 ll. the Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1-5.2(B),
- 24 et seq.;
- 25 mm. the South Carolina Unfair Trade Practices Act, S.C. Code Ann. §§ 39-5-
- 26 10, et seq.;
- 27 nn. the South Dakota Deceptive Trade Practices and Consumer Protection, S.D.
- 28 Codified Laws § 37-24-1, et seq.;

- 1 oo. the Tennessee Consumer Protection Act, Tenn. Code Ann. § 47-18-101, et seq.;
- 2 pp. the Texas Deceptive Trade Practices-Consumer Protection Act, Tex. Code Ann.,
- 3 Bus. & Con. § 17.41, et seq.;
- 4 qq. the Utah Consumer Sales Practices Act, Utah Code. Ann. § 13-11-175, et seq.;
- 5 rr. the Vermont Consumer Fraud Act, 9 V.S.A. § 2451, et seq.;
- 6 ss. the Virginia Consumer Protection Act of 1977, Va. Code Ann. § 59.1-199, et
- 7 seq.;
- 8 tt. the Washington Consumer Protection Act, Wash. Rev. Code § 19.86.010, et seq.;
- 9 uu. the West Virginia Consumer Credit And Protection Act, W. Va. Code § 46A, et
- 10 seq.;
- 11 vv. the Wisconsin Deceptive Trade Practices Act, Wis. Stat. § 100.18, et seq.; and
- 12 ww. the Wyoming Consumer Protection Act, Wyo. Stat. Ann. § 40-12-101, et seq.

13 162. The acts, practices, misrepresentations and omissions by Defendant described above,

14 and Defendant's dissemination of deceptive and misleading advertising and marketing materials in

15 connection therewith, occurring in the course of conduct involving trade or commerce, constitute

16 unfair methods of competition and unfair or deceptive acts or practices within the meaning of each of

17 the above-enumerated statutes.

18 163. Defendant's acts and practices described herein misled, deceived or damaged Plaintiffs

19 and Class members in connection providing the goods and services mentioned herein. Defendant's

20 conduct also constituted the use or employment of deception, fraud, false pretense, false promise,

21 misrepresentation, or knowingly concealing, suppressing, or omitting a material fact with intent that

22 others rely upon the concealment, suppression or omission in connection with the sale or

23 advertisement of goods or services whether or not a person has in fact been misled, deceived or

24 damaged in violation of each of the above-enumerated statutes.

25 164. Defendants knew or should have known that their conduct violated the above-

26 enumerated statutes. Defendants intended that the Plaintiffs and Class members would rely on their

27 misrepresentations, omissions, and concealment of information.

28

1 165. The foregoing acts, omissions, and practices proximately caused Plaintiff and Class
2 members to suffer damages as described herein.

3 166. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by
4 law, including damages stemming from Defendant's unfair, unlawful, and fraudulent business
5 practices or use of their PII; declaratory relief; reasonable attorneys' fees and costs; injunctive relief;
6 and other appropriate equitable relief.

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

9 168. Plaintiff has provided Defendants with notice of their violations of Code of Ala. § 8-19-
10 10, Alaska Stat. § 45.50.535, Cal. Civ. Code § 1782(a), Ga. Code Ann. § 10-1-399, 815 ILCS 505/10a,
11 Ind. Code Ann. § 24-5-0.5-5, Me. Rev. Stat. Ann. Tit. 5, § 213, Mass. Gen Laws Ann. Ch. 93A, Miss.
12 Code Ann. § 75-24-15, Tex. Bus. & Com. Code § 17.505, W. Va. Code § 46A-6-106, Wyo. Stat. §
13 40-12-109, and any other state consumer protection statute requiring notice to them of a claim for
14 damages. The notice was transmitted on the day this lawsuit and Amended Complaint were filed.
15 Plaintiffs initially bring a claim for injunctive or equitable relief under these particular statutes. After
16 the respective cure periods have expired and Defendants have failed to adequately address the
17 violations alleged herein, Plaintiff will amend the complaint to add a claim for damages under the
18 respective statutes.

19 **VIII. PRAYER FOR RELIEF**

20 WHEREFORE, Plaintiffs Joseph Martinez and Daniel Petro respectfully requests that this Court:

21 a. Certify this action as a class action, proper and maintainable pursuant to Rule 23 of the
22 Federal Rules of Civil Procedure; declare that Plaintiffs is a proper class representative; and appoint
23 Plaintiffs' counsel as Class Counsel;

24 b. Grant permanent injunctive relief to prohibit Defendant from continuing to engage in
25 the unlawful acts, omissions, and practices described herein;

26 c. Award Plaintiffs and Class members compensatory, consequential, general, and nominal
27 damages in an amount to be determined at trial;

28 d. Award statutory damages, trebled, and punitive or exemplary damages, to the extent

1 permitted by law;

2 e. Grant declaratory relief sought herein;

3 f. Award to Plaintiffs the costs and disbursements of the action, along with reasonable
4 attorneys' fees, costs, and expenses;

5 g. Award pre- and post-judgment interest at the maximum legal rate; and

6 h. Grant all such other relief as is just and proper.

7
8 **JURY DEMAND**

9 Pursuant to Fed. R. Civ. P. 38(b), Plaintiffs demands a trial by jury on all claims so triable.

10 Dated: April 15, 2020

Respectfully Submitted,

11 By: /s/ Jennie Lee Anderson

12 JENNIE LEE ANDERSON (SBN 203586)

13 jennie@andrusanderson.com

14 ANDRUS ANDERSON LLP

15 155 Montgomery Street, Suite 900

San Francisco, CA 94104

16 Telephone: (415) 986-1400

17 Facsimile: (415) 986-1474

18 Elizabeth A. Fegan (*pro hac vice forthcoming*)

19 beth@feganscott.com

20 FEGAN SCOTT LLC

150 S. Wacker Dr., 24th Floor

Chicago, IL 60606

21 Telephone: (312) 741-1019

22 Facsimile: (312) 264-0100

23 Lynn A. Ellenberger (*pro hac vice forthcoming*)

24 lynn@feganscott.com

25 FEGAN SCOTT LLC

500 Grant St., Suite 2900

Pittsburgh, PA 15219

26 Telephone: (412) 346-4104

27 Facsimile: (412) 785-2400

28 J. Barton Goplerud (*pro hac vice forthcoming*)

goplerud@sagwlaw.com

SHINDLER, ANDERSON,

GOPLERUD & WEESE, P.C.,

5015 Grand Ridge Drive, Suite 100

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

West Des Moines, IA 50265
Telephone: (515) 223-4567
Facsimile: (515) 223-8887

Attorneys for Plaintiffs