Adam J. Zapala (SBN 245748)
Reid Gaa (SBN 330141)
COTCHETT, PITRE & McCARTHY, LLP.
840 Malcolm Road, Suite 200
Burlingame, CA 94010
Tel: (650) 697-6000
Fax: (650) 697-0577
Emails: azapala@cpmlegal.com; rgaa@cpmlegal.com

Scott C. Nehrbass (*pro hac vice pending*)
Daniel J. Buller (*pro hac vice pending*)
FOULSTON SIEFKIN LLP
32 Corporate Woods, Suite 600
9225 Indian Creek Parkway
Overland Park, KS 66210-2000
Tel: (913) 253-2144
Fax: (866) 347-1472
Emails: snehrbass@foulston.com; dbuller@foulston.com

E. Powell Miller
Sharon S. Almonrode
THE MILLER LAW FIRM, P.C.
950 W. University Dr., Suite 300
Rochester, Michigan 48307
Telephone: (248) 841-2200
Fax: (248) 652-2852
Emails: epm@millerlawpc.com; ssa@millerlawpc.com

Counsel for Plaintiffs I.C., Amy Gitre, and the Putative Class

UNITED STATES DISTRICT COURT

DISTRICT OF CALIFORNIA

I.C., a minor, by and through his natural parent, NASIM CHAUDHRI, and AMY GITRE, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

ZYNGA, INC.,

Defendant.

Case No. _____

COMPLAINT

CLASS ACTION

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

I.C., a minor by and through his natural parent, Nasim Chaudhri, and Amy Gitre ("Plaintiffs"), individually and on behalf of a Class defined below of similarly situated persons, allege the following against Defendant Zynga, Inc., based upon personal knowledge and on information and belief derived from, among other things, Zynga's September 12, 2019 "Player Security Announcement," investigation of counsel, media reports, and review of public documents.

NATURE OF COMPLAINT

1. Plaintiffs bring this action against Zynga for its failure to reasonably safeguard Plaintiffs' Personally Identifiable Information ("PII") as defined herein, failure to reasonably provide timely notification that Plaintiffs' PII had been accessed and acquired by an unauthorized third party through a data breach, and for intentionally and unconscionably deceiving Plaintiffs relating to the status, safety, location, access, and protection of Plaintiffs' PII.

2. As a result of Zynga's negligent, intentional, or unconscionable failure to adequately satisfy its statutory and common-law obligations, Plaintiffs' PII was accessed, acquired, and stolen for the purpose of misusing Plaintiffs' data and causing further irreparable harm to Plaintiffs' personal, financial, reputational, and future well-being. After the theft of Plaintiffs' PII from Zynga's platform, it was distributed to and among hacker forums and other identity and financial thieves for the purpose of illegally misusing, reselling, and stealing Plaintiffs' PII and identity. Plaintiffs have been damaged as a result.

3. Plaintiffs bring this lawsuit against Zynga for statutory violations as well as common law tort claims under negligence, negligent misrepresentation, negligence per se, unjust enrichment, violation of state data breach statutes, intrusion upon seclusion, and declaratory judgment.

4. As used throughout this Complaint, "PII" is defined to include all information exposed by the Zynga data breach; all information so defined under individual states' statutes; and all or any part or combination of name, address, birth date, Social Security number, driver's license information (any part of license number, state, home address, dates of issuance or expiration), telephone number, email address, tax identification number, credit card number,

usernames, passwords, and log-in information that can be used to access a person's personal electronic content.

PARTIES

5. Zynga, Inc. is a Delaware corporation with its principal place of business in San Francisco, California.

6. Plaintiff I.C., a minor, by and through his natural parent, Nasim Chaudhri, is an individual citizen of Kansas who had a Zynga account at the time of the incidents described herein and entrusted PII to Zynga with the reasonable expectation and understanding that Zynga would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized users and would be timely and forthright relating to any data security incidents involving Plaintiffs' PII.

7. Plaintiff Amy Gitre is an individual citizen of Michigan who had a Zynga account at the time of the incidents described herein and entrusted PII to Zynga with the reasonable expectation and understanding that Zynga would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized users and would be timely and forthright relating to any data security incidents involving Plaintiffs' PII.

8. The class members are all adults and minor individuals in the United States whose PII was obtained or maintained by Zynga and compromised as a result of the Zynga data breach described herein.

JURISDICTION

9. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, the number of class members exceeds 100, and Zynga is a citizen of a State different from that of at least one Class member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

10. This Court has personal jurisdiction over Zynga because it is authorized to and regularly conducts business in California and is headquartered in San Francisco, California.

VENUE

11. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this district.

INTRADISTRICT ASSIGNMENT

12. Assignment is appropriate in the San Francisco Division because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in San Francisco County.

GENERAL ALLEGATIONS

I. Zynga – Background.

13. Zynga is a social game developer and host that develops, markets, and operates social games played on the internet, social networking sites, Zynga.com, and mobile platforms such as iPhones and Android devices. Zynga also provides advertising services to advertising agencies and brokers.[1]

14. Zynga operates popular games such as Words With Friends, Words With Friends 2, Zynga Poker, CSR Racing, Empires & Puzzles, Merge Dragons, and others.

15. Users can purchase Zynga's games, which are for sale through mobile marketplaces such as the iTunes Store or the Google Play Store (formerly known as the Android Market). Alternatively, Zynga has offered at least some of its games in exchange for increased in-game advertising and potentially other consideration such as sale of in-game virtual goods—as well as its users' valuable PII.

16. One of Zynga's most popular offerings is Words With Friends, a game released in 2009 that resembles two-player Scrabble in a crossword-puzzle style.[2] Up to 40 simultaneous Words With Friends games can be played by each user spread across the nation who have the ability to compete against each other and communicate using the game's built-in chat feature.[3]

17. Between 2010 and 2011, Words With Friends was one of the top-ranked games in

[1] https://www.crunchbase.com/organization/zynga#section-overview (last visited Jan. 14, 2020).

[2] https://en.wikipedia.org/wiki/Words_with_Friends (last visited Jan. 14, 2020).

[3] https://en.wikipedia.org/wiki/Words_with_Friends (last visited Jan. 14, 2020).

the Apple Store, and the game continued to be popular for years. In fact, Words With Friends was the #1 most popular Apple (iOS-based) game in all of 2016. And as of March 2017, Words With Friends remained the most popular game in the United States with 13 million unique users for that month.[4]

18. Zynga's business of exchanging mobile gaming for, in part, its massive user database of PII, has been wildly successful. Zynga posted revenue of $1.28 billion in 2012, and earned more than $900 million in 2018.[5] According to recent statements by the company's CEO, Zynga's success is likely to continue as it "is on track to be one of the fastest-growing—if not the fastest-growing—gaming company at scale."[6] Zynga's stock "soared 56% in 2019,"[7] and it finished the first week of February 2020 at a 52-week high.[8]

II. Zynga collects personally identifiable information from its users.

19. Zynga requires all individuals who wish to access games on its website to create a Zynga user account, which requires the user to submit certain information to Zynga. The user can create an account with Zynga through the user's email address or through the user's Facebook account.

20. At this time, the information that Zynga requires for prospective users to become active users initially includes the user's first name, last name, email address, a password, and the user's gender.

21. Zynga does not require prospective users to provide their age or date of birth.

22. Zynga collects its users' names, email addresses, login IDs, password reset tokens,

[4] https://www.pocketgamer.biz/news/65662/words-with-friends-13-million-users-march-2017/ (last visited Jan. 14, 2020; https://en.wikipedia.org/wiki/Words_with_Friends (last visited Jan. 14, 2020).

[5] https://www.statista.com/statistics/273567/zyngas-annual-revenue/ (last visited Jan. 14, 2020).

[6] https://www.bloomberg.com/news/articles/2020-01-03/zynga-is-booming-again-after-wilderness-years-at-farmville-maker (last visited Jan. 14, 2020).

[7] https://www.fool.com/investing/2020/01/08/why-zynga-stock-soared-56-in-2019.aspx (last visited Jan. 14, 2020).

[8] https://www.fool.com/investing/2020/02/08/3-surprising-stocks-hitting-new-highs-this-week.aspx

Facebook IDs, Zynga account IDs, and passwords, among other pieces of information.

23. If a prospective mobile user chooses to log in with Facebook, the prospective user must provide their Facebook username and password.

III. Many of Zynga's users are minors.

24. One of Zynga's principal targeted demographics is minor children like Plaintiff I.C.

25. Zynga does not publicly disclose its user demographics, but one study estimates that 8% of all mobile gamers are minor children.[9]

26. If just 8% of Zynga users are minors, that means nearly 14 million children were victims of the September 2019 data breach. In light of the nature of Zynga's available games, the number of affected minors is likely to be much higher in this case.

27. The actual percentage of Zynga's user base that are minors is likely to be significantly higher than the average. Zynga has known that it is subject to governmental regulation for "the collection of data from minors" for a number of years.[10] In its 2016 10-K, Zynga acknowledged that it is subject to these regulations and stated that "We [Zynga] receive, store, and process personal information and other player data . . . ."[11]

28. Zynga does not require users to verify their age during the registration process.

29. On information and belief, and based on reporting in the media, Zynga is well-aware that a substantial portion of its user base has historically been, and continues to be, comprised of minors, and Zynga has profited handsomely from that user base over the years.

---

[9] https://www.adcolony.com/blog/2019/08/14/breaking-down-mobile-gaming-demographics/ (last visited December 23, 2019)

[10] Zynga's 2016 Form 10-K, https://www.sec.gov/Archives/edgar/data/1439404/000156459017001775/znga-10k_20161231.htm (last visited Jan. 14, 2020). *See also* Zynga's 2019 Form 10-K, https://investor.zynga.com/static-files/0ebaee4f-8d78-4faf-8b71-95a23c4c3995 (last visited Jan. 14, 2020).

[11] Zynga's 2016 Form 10-K, https://www.sec.gov/Archives/edgar/data/1439404/000156459017001775/znga-10k_20161231.htm (last visited Jan. 14, 2020). *See also* Zynga's 2019 Form 10-K, https://investor.zynga.com/static-files/0ebaee4f-8d78-4faf-8b71-95a23c4c3995 (last visited Jan. 14, 2020).

30. For example, a January 2019 article published in *Popular Mechanics* entitled "Documents Show Facebook Knowingly Took Money from Unwitting Children," states that games such as "Zynga's PetVille" "are free to download but come packed with opportunities to spend actual money to advance further. These cash payments are meant to look like items within the game, and it's not easy for a child not to realize what they're doing."[12]

31. In fact, one 12-year-old user of a Zynga game had "emptied his own savings account" and then used his mother's credit in accruing many hundreds of dollars in charges.[13] Zynga refused to refund the charges.[14]

32. Based on their status as minors, Plaintiff I.C. and the Class of minors are not bound by any contractual terms that Zynga may try to force upon its users during the registration process or at any other time thereafter.

33. I.C. hereby disaffirms Zynga's Terms of Service and Privacy Policy.

IV. Minors are a high-value target for cyber criminals and are particularly vulnerable to long-term identity theft and PII misuse.

34. According to numerous media reports and studies, stealing the identity of minors is especially attractive to cyber criminals for a host of reasons, including: (1) minors' credit reports are clean, which makes them particularly valuable; (2) minors do not check their credit reports or review monthly bills the way adults do; (3) thieves are more likely to have unfettered access to minors' identity and credit for years or even decades; (4) it is often difficult or impossible to place a freeze on a minor's credit report—because they don't yet *have* credit; and (5) minors are less likely to receive notice, or to have an opportunity to take notice in the event

---

[12] https://www.popularmechanics.com/technology/apps/a26041842/documents-show-facebook-knowingly-took-money-from-unwitting-children/ (last visited Jan. 14, 2020). *See also* revealnews.com, *Facebook knowingly duped game-playing kids and their parents out of money*, https://www.revealnews.org/article/facebook-knowingly-duped-game-playing-kids-and-their-parents-out-of-money/ (last visited Jan. 14, 2020) (stating that such conduct by Zynga's PetVille was "friendly fraud" and that "the children did not even know they were spending money").

[13] https://www.theguardian.com/money/2010/apr/07/farmville-user-debt-facebook (last visited Jan. 14, 2020).

[14] *Id.*

that identity theft occurs or is ongoing, such as, e.g., if fraudulent accounts or charges occur under their names, if fake tax returns are filed in their names, if fraudulent health care is obtained under their identity, and if their information is fraudulently used in connection with employment.[15]

35. The Federal Trade Commission agrees that when children are victims of a data breach "it might be years before you or your child realizes there's a problem."[16]

36. For these and other reasons, identity theft is a growing problem in the United States as it relates to our minor population. More than 1 million minors were victims of identity theft or fraud in 2017, totaling $2.6 billion in fraudulent activity.[17]

37. In fact, in 2017, among notified breach victims, 39% of minors became victims of actual fraud (as opposed to 19% of adults).[18]

38. According to a report on child identity theft published by Carnegie Mellon, a study based on identity protection scans of 40,000 U.S. children, the risk that someone was using their social security number was 51 times higher than the rate for adults in the same population.[19]

39. The Carnegie Mellon report continues: "[t]he potential impact [of identity theft] on the child's future is profound; it could destroy or damage a child's ability to win approval on student loans, acquire a mobile phone, obtain a job, or secure a place to live."[20]

40. Based on the common use of mobile games among minors, Zynga was well aware

---

[15] https://www.nytimes.com/2015/04/18/your-money/a-childs-vulnerability-to-identity-theft.html (last visited December 23, 2019).

[16] https://www.consumer.ftc.gov/blog/2015/10/protecting-your-childs-information-after-data-breach (last visited February 20, 2020).

[17] https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html (last visited December 23, 2019); see also https://www.nbcnews.com/business/consumer/more-1-million-children-were-victims-id-theft-last-year-n885351 (last visited December 23, 2019).

[18] https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html (last visited December 23, 2019).

[19] https://www.cylab.cmu.edu/_files/pdfs/reports/2011/child-identity-theft.pdf, at PDF p. 4 (last visited December 23, 2019).

[20] https://www.cylab.cmu.edu/_files/pdfs/reports/2011/child-identity-theft.pdf, at PDF p. 3 (last visited December 23, 2019).

of the economic and reputational value of exploiting children for its own monetary gain, and it should have been equally concerned with protecting the PII entrusted to it by that valuable and relatively defenseless group.

V. Zynga's substandard password security; the resulting data breach; and Zynga's subsequent failure to reasonably respond and to adequately notify users.

41. In September 2019, hacker Gnosticplayers ("Hacker") told the *The Hacker News* that he breached Zynga's user database, gaining access to more than 218 million user accounts.[21]

42. The Hacker said that the stolen information included names, email addresses, login IDs, password reset tokens, Facebook IDs, Zynga account IDs, and passwords secured with SHA-1 cryptography, an encryption method that "has been considered outdated and insecure since before Zynga was even founded."[22]

43. According to reports, the data breach is known to have included at least the following Zynga games: Words With Friends; Draw Something; and OMGPOP.

44. The OMGPOP breach allegedly exposed clear text passwords for over 7 million users.

45. The Hacker "is a known quantity in the digital criminal underground, having been observed selling hundreds of millions of breached accounts on the dark web since early 2019."[23] Media reports state that the Hacker has sold stolen account information from other data breaches on the dark web on at least five occasions involving more than one billion user credentials and personal details.[24]

46. On September 12, 2019, Zynga posted a "Player Security Announcement" on its

---

[21] https://thehackernews.com/2019/09/zynga-game-hacking.html (last visited December 23, 2019).

[22] https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/ (last visited Jan. 4, 2020).

[23] https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/ (last visited Jan. 4, 2020).

[24] https://cyware.com/news/times-when-gnosticplayers-hacker-made-headlines-for-selling-troves-of-stolen-data-on-dark-web-f8849502 (last visited Jan. 14, 2020).

website stating that it "recently discovered that certain player account information may have been illegally accessed by outside hackers."[25]

47. Rather than taking responsibility for its cybersecurity shortcomings, Zynga's Player Security Announcement implied that data breaches are impossible to avoid. The first sentence of the Player Security Announcement says that "Cyber attacks are one of the unfortunate realities of doing business today."[26]

48. Zynga did not, and has not to this day, issued an email notification of the breach to its users. Rather, Zynga effectively hid the fact that it suffered a data breach. Only those users who happened to visit Zynga's website on their own volition, read about the breach in the news, or had signed up to receive email data breach notifications from independent third parties that monitor data breaches were made aware of the breach.

49. Zynga had the ability to send an email notification to all users because providing an email address appears to be a universal requirement Zynga imposes on all users when going through the registration process.

50. Rather than sending an email to all users at the time of the breach, Zynga spent its time shoring up its legal defenses.

51. Some Zynga users first learned of the breach through receipt of an email alert from the website "Have I Been Pwned," which allows users to sign up for notifications when their PII is included in a data breach. That alert was not sent until December 18, 2019. The unfortunate reality is that most Zynga users are still completely unaware that their PII was stolen as a result of the Zynga data breach, because Zynga failed to reasonably advise them.

52. In light of the amount of time that has passed since the data breach, it is "likely that the stolen passwords have been decrypted." That fact, coupled with Zynga's failure to notify its users, places them at increased risk. As noted by one prominent cybersecurity expert: "The

[25] https://investor.zynga.com/news-releases/news-release-details/player-security-announcement (last visited Dec. 23, 2019).

[26] https://investor.zynga.com/news-releases/news-release-details/player-security-announcement (last visited Dec. 23, 2019).

disclosure of the full scale and nature of this breach, some three months after the initial announcement, is concerning. This delay, and the initial lack of information provided by Zynga to its users, has put victims at unnecessary risk."[27]

53. Zynga's conduct leading up to and following the data breach show it is far more concerned with protecting itself than with safeguarding the valuable and confidential information of its users. As noted by one industry expert: "Zynga's response to its breach demonstrates how some organizations tend to view proper security as an afterthought."[28]

54. Zynga released an updated version of its Terms of Service and Privacy Policy on December 18, 2019, the very same day the notification was issued from *Have I Been Pwned*, but still did not send an email to Zynga users alerting them of the breach.

55. The PII stolen from Zynga constitutes "personal identifying information," which qualifies as "identity theft" when used to defraud or otherwise misrepresent with the intent of harming the owner of the information. Identity theft can occur by using (with the intent to defraud) information such as: name, birth date, address, phone number, passwords, usernames, or other log-in information that can be used to access a person's electronic content, including content stored on a social networking site.[29]

56. The information stolen from Zynga included names, phone numbers, usernames, email addresses, and passwords—PII that is highly valued amongst cyber thieves and criminals on the Dark Web. For example, Apple ID usernames and passwords were sold on average for $15.39 each on the Dark Web, making them the most valuable non-financial credentials for sale on that marketplace. Usernames and passwords for eBay ($12), Amazon (≤$10), and Walmart (≤$10) are not far behind. In fact, there is a well-established market for stolen account credentials on the Dark Web, which includes Zynga credentials.

---

[27] https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/ (last visited Jan. 4, 2020).

[28] https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/ (last visited Jan. 4, 2020).

[29] *See* K.S.A. 21-6107(2).

57. As stated above, the Hacker obtained over 200 million passwords, including more than 7 million passwords that Zynga had stored in clear text, as a result of the data breach.

58. Passwords that are stored using "SHA1," Zynga's chosen encryption method, are only slightly safer: "Security experts have long warned that SHA1 is not fit for protecting passwords because it's so easy to crack. As a result, any organization that continues to use SHA1 should be viewed as having substandard security practices in place, and by extension not taking seriously the security of its customer data."[30]

59. The Hacker also obtained millions of email addresses and usernames.

60. This combination of usernames, email addresses, and easily deciphered passwords makes the contents of the breach valuable to thieves and increases the chances of identity theft.

61. In part, the danger comes from password reuse and a process known as credential stuffing.

62. Troy Hunt, a cyber security expert and the founder of *Have I Been Pwned*, described the password reuse issue in 2017:

> So there's a lot of stuff getting hacked and a lot of credentials floating around the place, but then what? I mean what do evil-minded people do with all those email addresses and passwords? Among other things, they attempt to break into accounts on totally unrelated websites. Here's a great example: someone grabs the 164 million record LinkedIn data dump that turned up last year and cracks the hashes. They're SHA1 without a salt so the protection on the passwords is pretty useless. In no time at all you've got tens of millions of email address and plain text password pairs. And this is where the real problems begin.
>
> As fallible humans, we reuse passwords. We've all done it at one time or another and whilst I hope that by virtue of you being here reading security stuff you've got yourself a good password manager, we've all got skeletons in our closets (more on mine soon). Most people are just out there YOLO'ing away with the same password or three across all their things. We know that because again, we've all done it and hackers know that because that's their job! As such, they're going to try and break into as many other accounts as they can using the credentials from a data breach.[31]

63. Credential stuffing is a process through which large numbers of username and password pairs are entered into websites other than the breached website until a hacker can access

[30] https://www.bankinfosecurity.com/blogs/zyngas-breach-notification-how-to-inform-victims-p-2796 (Last visited December 23, 2019)

[31] https://www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned/ (Last visited December 23, 2019).

and hijack accounts.[32]

64. Mr. Hunt further states that credential stuffing is a serious threat because: (1) "It's enormously effective due to the password reuse problem"; (2) "It's hard for organisations to defend against because a successful 'attack' is someone logging on with legitimate credentials"; (3) "It's very easily automatable; you simply need software which will reproduce the logon process against a target website"; and (4) "There are readily available tools and credential lists that enable anyone to try their hand at credential stuffing."

65. In addition to credential stuffing, the breached data includes "enough information for hackers to potentially create targeted phishing attacks made up to look as if they are an official communication from Zynga."[33]

66. The stolen information "is sure to find a home on the dark web, enabling fraudsters to log into user accounts and commit account takeover fraud."[34] Also, "[b]ecause [Zynga] games are often connected to user Facebook accounts, hackers can gain access to far more information under a forged identity."[35] "According to BuiltWith, there are over 190,000 websites that are Facebook Login Button customers and almost 40,000 live websites using Facebook Login Button. Logging in with this stolen information (including the 7 million Draw Something passwords left in clear text with this breach) makes it impossible to determine if the actual account holder is the one logging in."[36]

67. In this case, the stolen information was provided to the data breach monitoring website, *Have I Been Pwned*,[37] which added the Zynga database to its website so users can check

---

[32] https://www.owasp.org/index.php/Credential_stuffing (last visited December 23, 2019).

[33] https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/ (last visited Jan. 4, 2020).

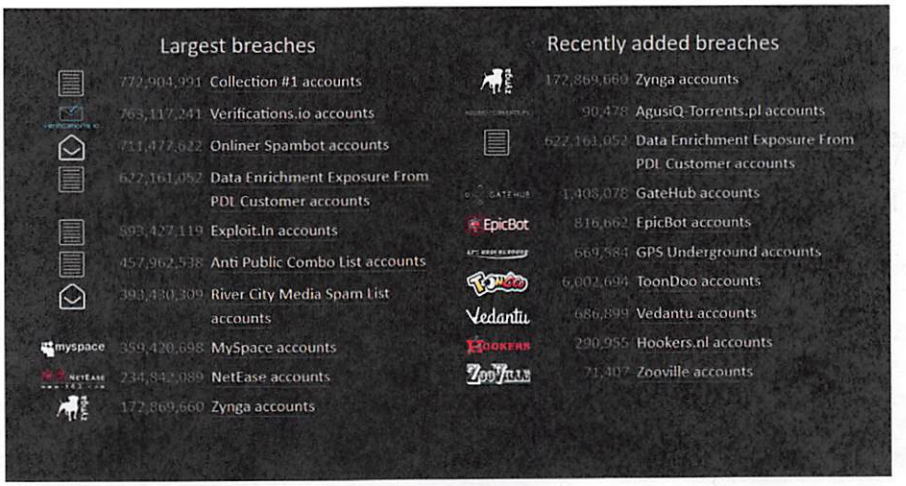
[34] https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/ (last visited Jan. 4, 2020).

[35] https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/ (last visited Jan. 4, 2020).

[36] https://www.cpomagazine.com/cyber-security/password-breach-of-game-developer-zynga-compromises-170-million-accounts/ (last visited Jan. 4, 2020).

[37] https://haveibeenpwned.com/ (pronounced "poned") (Last visited, December 2019).

to see if their email was included in the breach. As shown in the below screenshot from *Have I Been Pwned*, 172,869,600 accounts were stolen from Zynga, which makes it ***the tenth-largest data breach of all time***.



68. A search of *Have I Been Pwned* confirms that Plaintiffs' information was exposed as a result of the Zynga data breach.[38]

69. Plaintiffs' and the Class's PII was among the confidential information compromised in the Zynga data breach, causing Plaintiffs and the Class to suffer injury and damages, including but not limited to: the improper disclosure of the PII; the loss of the value of the PII; ongoing disclosures and dissemination of the PII; the imminent threat of identity theft and other fraud against Plaintiffs and the Class; the loss of Plaintiffs' and the Class's privacy; and out-of-pocket expenses and time devoted to mitigating the effects of the data breach and ascertaining the extent of Plaintiffs' and the Class's losses and exposure.

70. Plaintiffs and the Class would never have provided their PII to Zynga if the deficient security provided by Zynga was known and understood.

71. Plaintiffs and the Class would further never have provided their PII to Zynga if they had known that Zynga would fail to properly inform Plaintiffs and the Class in the event that Zynga experienced a data breach.

72. Plaintiffs and the Class would never have provided their PII to Zynga if Zynga had

[38] https://www.bleepingcomputer.com/news/security/database-from-Zynga-hack-sold-online-check-if-youre-included/ (Last visited, August 2019) (Exhibit 23).

disclosed that it lacked adequate security measures and data security practices, as was revealed by the media reports.

73. Plaintiffs and the Class have been damaged in that they spent time and resources, and will spend additional time and resources in the future, speaking with representatives; researching and monitoring accounts; researching and monitoring credit history; responding to identity theft incidents; purchasing identity protection; and suffering annoyance, interference, and inconvenience, as a result of the data breach.

74. Zynga's actions and failures to act when required have caused Plaintiffs and the Class to suffer harm and face the significant and imminent risk of future harm, including but not limited to:

- theft of their PII;
- costs associated with researching the scope and nature of the breach and of responding to the data breach and attendant risks and harm in light of Zynga's failure to adequately notify;
- costs associated with the detection and prevention of identity theft and unauthorized use of their PII;
- unauthorized access to and misuse of their online accounts;
- lowered credit scores resulting from credit inquiries and caused by fraudulent activities;
- costs associated with time spent and the loss of productivity from taking time to address ameliorate, mitigate, and deal with the actual and future consequences of the Zynga data breach—including finding fraudulent charges and enrolling in and purchasing credit monitoring and identity theft protection services;
- the imminent and impending injury flowing from potential fraud and identify theft posed by their Personal Information being placed in the hands of criminals;
- damages to and diminution in value of their PII entrusted, directly or

indirectly, to Zynga with the mutual understanding that Zynga would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others; and

- continued risk of exposure to hackers and thieves of their PII, which remains in Zynga's possession and is subject to further breaches so long as Zynga fails to undertake appropriate and adequate measures to protect Plaintiffs and the Class.

75. Consequently, Plaintiffs and the Class are at an imminent risk of fraud, criminal misuse of their PII, and identity theft for years to come as result of the data breach and Zynga's deceptive and unconscionable conduct.

CLASS ALLEGATIONS

76. Plaintiffs bring this action on behalf of adults and minors similarly situated both across the United States and within their State or Territory of residence.

77. Class certification is appropriate under Fed. R. Civ. P. 23(a) and (b)(1), (b)(2), and/or (b)(3).

78. **Nationwide Class:** All individuals in the United States whose PII was obtained or maintained by Zynga and compromised as a result of the Zynga data breach described herein.

79. **Nationwide Adult Subclass:** All adult individuals in the United States whose PII was obtained or maintained by Zynga and compromised as a result of the Zynga data breach described herein.

80. **Nationwide Minor Subclass:** All minor individuals in the United States whose PII was obtained or maintained by Zynga and compromised as a result of the Zynga data breach described herein, as well as all individuals in the United States who provided their PII to Zynga while they were minors and had their PII compromised as a result of the Zynga data breach described herein.

81. The Nationwide Class, Nationwide Adult Subclass, and Nationwide Minor Subclass are collectively referred to herein as the "Class."

82. **Numerosity (FRCP 23(a)(1)):** The Class satisfies the numerosity requirement

because it is composed of millions of persons, in numerous locations. The number of class members is so large that joinder of all its members is impracticable.

83. **Commonality and Predominance (FRCP 23(a)(2) and 23(b)(3)):** There are questions of law and fact common to the Class, and these questions predominate over questions affecting only individual Class members. Common legal and factual questions include, but are not limited to:

- whether the data breach constitutes a breach of the data-security commitments and obligations to protect and safeguard PII made to the Class by Zynga in its privacy policy;
- whether Zynga acted with intent or reckless indifference with respect to the Class and the safety, value, and security of the Class's PII when it merely posted a Player Security Announcement on its website rather than emailing users about the breach and taking other actions to mitigate;
- whether Zynga's conduct and practices described herein amount to acts of intrusion upon seclusion under the laws of the "Intrusion Upon Seclusion States" defined below;
- whether Zynga was negligent in establishing, implementing, and following security protocols;
- whether Zynga failed to abide by all applicable legal requirements (including relevant state law requirements) and industry standards concerning the privacy and confidentiality of the Class members' PII;
- whether the Class members' PII was compromised and exposed as a result of the data breach and the extent of that compromise and exposure;
- whether the Class members are entitled to compensatory damages;
- whether the Class members are entitled to injunctive relief; and
- whether the Class members are entitled to punitive damages.

84. **Typicality (FRCP 23(a)(3)):** Plaintiffs' claims are typical of the claims of the members of the Class because Plaintiff's claims, and the claims of all Class members, arise

out of the same conduct, policies, and practices of Zynga, as alleged herein, and all members of the Class are similarly affected by Zynga's wrongful conduct and the data breach described herein.

85. **Adequacy of Representation (FRCP 23(a)(4)):** Plaintiffs will fairly and adequately represent the Class and have retained counsel competent in the prosecution of class action litigation; data breach litigation; data privacy and cybersecurity law; and technical I.T. concepts, practices, and theory. Plaintiffs have no interests antagonistic to those of other members of the Class. Plaintiffs are committed to the vigorous prosecution of this action and anticipate no difficulty in the management of this litigation as a class action.

86. Class action status in this action is warranted under Rule 23(b)(1)(A) because prosecution of separate actions by the members of the Class would create a risk of establishing incompatible standards of conduct for Defendants. Class action status is also warranted under Rule 23(b)(1)(B) because prosecution of separate actions by the members of the Class would create a risk of adjudications with respect to individual members of the Class that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

87. In the alternative, certification under Rule 23(b)(2) is warranted because Defendants acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive, declaratory, or other appropriate equitable relief with respect to the Class as a whole.

88. In the alternative, certification under Rule 23(b)(3) is appropriate because questions of law or fact common to members of the Class predominate over any questions affecting only individual members, and class action treatment is superior to the other available methods for the fair and efficient adjudication of this controversy.

CAUSES OF ACTION AND CLAIMS FOR RELIEF

COUNT I — Negligence
(On behalf of Plaintiffs, the Nationwide Class, the Nationwide Adult Subclass, and the Nationwide Minor Subclass)

89. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

90. This count is brought on behalf of all Class members.

91. Zynga owed a duty to Plaintiffs and the Class to use and exercise reasonable and due care in obtaining, retaining, and securing their PII that Zynga collected.

92. Zynga owed a duty to Plaintiffs and the Class to provide security, consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the PII that Zynga collected.

93. Zynga owed a duty to Plaintiffs and the Class to implement processes to quickly detect a data breach, to timely act on warnings about data breaches, and to inform the Class of a data breach as soon as possible after it is discovered.

94. Zynga owed a duty of care to Plaintiffs and the Class because they were a foreseeable and probable victim of any inadequate data security practices.

95. Zynga solicited, gathered, and stored the PII provided by Plaintiffs and the Class.

96. Zynga knew or should have known it inadequately safeguarded this information.

97. Zynga knew or should have known that a breach of its systems would inflict millions of dollars of damages upon Plaintiffs and the Class, and Zynga was therefore charged with a duty to adequately protect this critically sensitive information.

98. Zynga had a special relationship with Plaintiffs and the Class. Plaintiffs' and the Class's willingness to entrust Zynga with their PII was predicated on the understanding that Zynga would take adequate security precautions. Moreover, only Zynga had the ability to protect its systems and the PII it stored on them from attack.

99. Zynga's conduct also created a foreseeable risk of harm to Plaintiffs and the Class and their PII. Zynga's misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

100. Zynga breached the duties it owed to Plaintiffs and the Class by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiffs and the Class.

101. Zynga breached the duties it owed to Plaintiffs and the Class by creating a foreseeable risk of harm through the misconduct previously described.

102. Zynga breached the duties it owed to Plaintiffs and the Class by failing to properly implement technical systems or security practices that could have prevented the loss of the data at issue.

103. Zynga breached the duties it owed to Plaintiffs and the Class by failing to timely, adequately, and accurately disclose that Plaintiffs' and the Class members' PII had been improperly stolen, acquired, or accessed.

104. The law further imposes an affirmative duty on Zynga to timely disclose the unauthorized access and theft of the PII to Plaintiffs and the Class so that Plaintiffs and the Class can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their financial and sensitive information.

105. Zynga breached its duty to notify Plaintiffs and the Class by failing to provide Plaintiffs and the Class with information regarding the breach beyond the inadequate Player Security Update posted on its website. To date, Zynga has not provided sufficient information to Plaintiffs and the Class regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and the Class.

106. As a direct and proximate result of Zynga's negligent conduct, Plaintiffs and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II - Negligence
(On behalf of I.C. and the Nationwide Minor Subclass)

107. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

108. This count is brought on behalf of I.C. and the Nationwide Minor Subclass.

109. I.C. and the Nationwide Minor Subclass are one of Zynga's principal targeted demographics and account for a sizeable portion of Zynga's total user base, and Zynga has long been aware of that fact.

110. I.C. and the Nationwide Minor Subclass are a particularly vulnerable and defenseless group of Zynga users and are more significantly damaged and imminently threatened

to be damaged as a result of Zynga's negligence described herein because, without limitation, they are especially: (1) attractive targets to cyber criminals; (2) vulnerable to fraudulent activity and identity theft with respect to their stolen PII; (3) defenseless to protect themselves from such theft, fraud, or identity theft; and (4) subject to prolonged surreptitious fraud and identity theft following the theft of their data, all of which is well documented in academic and government-issued materials, by experts in the field, and by the media.

111. Zynga owed a heightened duty to I.C. and the Nationwide Minor Subclass to use and exercise reasonable and due care in obtaining, retaining, and securing their PII that Zynga collected, and Zynga was aware of the heightened vulnerability and damage that would be suffered by I.C. and the Nationwide Minor Subclass in the event of a data breach.

112. Zynga owed a heightened duty to I.C. and the Nationwide Minor Subclass to provide security, consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the minors' PII that Zynga collected.

113. Zynga owed a heightened duty to I.C. and the Nationwide Minor Subclass to implement processes to quickly detect a data breach, to timely act on warnings about data breaches, and to inform the Class of a data breach as soon as possible after it is discovered.

114. Zynga owed a heightened duty to I.C. and the Nationwide Minor Subclass because they were foreseeable and probable victims of any inadequate data security practices.

115. Zynga solicited, gathered, and stored the PII provided by I.C. and the Nationwide Minor Subclass and profited from the same.

116. Zynga knew or should have known it inadequately safeguarded this information.

117. Zynga knew or should have known that a breach of its systems would inflict millions of dollars of damages upon I.C. and the Nationwide Minor Subclass, and Zynga was therefore charged with a heightened duty to adequately protect this critically sensitive information.

118. Zynga had a special relationship with I.C. and the Nationwide Minor Subclass; I.C. and the Nationwide Minor Subclass's willingness to entrust Zynga with their PII was predicated

on the understanding that Zynga would take adequate security precautions. Moreover, only Zynga had the ability to protect its systems and the PII it stored on them from attack and Zynga knew of the lack of sophistication and defenselessness of I.C. and the Nationwide Minor Subclass in taking steps to protect themselves in the event of a data breach.

119. Zynga's own conduct also created a foreseeable risk of harm to I.C. and the Nationwide Minor Subclass and their sensitive information. Zynga's misconduct included failing to: (1) secure its systems, despite knowing their unique vulnerabilities, (2) comply with industry standard security practices for protecting minors' PII, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

120. Zynga breached its heightened duties to I.C. and the Nationwide Minor Subclass by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the financial information of I.C. and the Nationwide Minor Subclass.

121. Zynga breached its heightened duties to I.C. and the Nationwide Minor Subclass by creating a foreseeable risk of harm through the misconduct previously described.

122. Zynga breached its heightened duties to I.C. and the Nationwide Minor Subclass by failing to properly implement technical systems or security practices that could have prevented the loss of the data at issue.

123. Zynga breached its heightened duties to I.C. and the Nationwide Minor Subclass by failing to timely, adequately, and accurately disclose that I.C. and the Nationwide Minor Subclass's PII had been improperly stolen, acquired, or accessed.

124. The law further imposes a heightened affirmative duty on Zynga to timely disclose the unauthorized access and theft of the PII to I.C. and the Nationwide Minor Subclass so that I.C. and the Nationwide Minor Subclass can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their financial and sensitive information.

125. Zynga breached its heightened duty to notify I.C. and the Nationwide Minor Subclass by failing to provide I.C. and the Nationwide Minor Subclass with information

regarding the breach beyond the inadequate Player Security Update posted on its website. To date, Zynga has not provided sufficient information to I.C. and the Nationwide Minor Subclass regarding the extent of the unauthorized access and continues to breach its disclosure obligations to I.C. and the Nationwide Minor Subclass.

126. As a direct and proximate result of Zynga's negligent conduct, I.C. and the Nationwide Minor Subclass have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III – Negligent Misrepresentation
(On behalf of Plaintiffs, the Nationwide Class, the Nationwide Adult Subclass, and the Nationwide Minor Subclass)

127. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

128. This count is brought on behalf of all Class members.

129. Through its Privacy Policy and other actions and representations, Zynga held itself out to Plaintiffs and the Class as possessing and maintaining adequate data security measures and systems that were sufficient to protect the PII belonging to Plaintiffs and the Class.

130. Zynga owed a duty to Plaintiffs and the Class to communicate accurate information about its compliance with the representations made in its Privacy Policy and about any material weaknesses in its data security systems and procedures.

131. Zynga knew or should have known that it was not in compliance with the representations made in its Privacy Policy.

132. Zynga knowingly and deliberately failed to disclose material weaknesses in its data security systems and procedures that good faith and common decency required it to disclose to Plaintiffs and the Class.

133. Neither Plaintiffs nor the Class could have known or discovered the material weaknesses in Zynga's data security practices.

134. A reasonable business would have disclosed information concerning material weaknesses in its data security measures and systems to Plaintiffs and the Class.

135. Zynga also failed to exercise reasonable care when it failed to properly communicate information concerning the data breach that it knew, or should have known,

compromised PII of Plaintiffs and the Class.

136. Plaintiffs and the Class justifiably relied on Zynga's representations, or lack thereof, when they provided their PII to Zynga.

137. As a direct and proximate result of Zynga's negligent misrepresentations by omission, Plaintiffs and the Class have suffered injury, have been damaged as described herein, and are entitled to damages in an amount to be proven at trial.

COUNT IV – Negligent Misrepresentation
(On behalf of I.C. and the Nationwide Minor Subclass)

138. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

139. This count is brought on behalf of I.C. and the Nationwide Minor Subclass.

140. I.C. and the Nationwide Minor Subclass are one of Zynga's principal targeted demographics and account for a sizeable portion of Zynga's total user base, and Zynga has long been aware of that fact.

141. I.C. and the Nationwide Minor Subclass are a particularly vulnerable and defenseless group of Zynga users and are more significantly damaged and imminently threatened to be damaged as a result of Zynga's negligent misrepresentation described herein because, without limitation, they are especially: (1) attractive targets to cyber criminals; (2) vulnerable to fraudulent activity and identity theft with respect to their stolen PII; (3) defenseless to protect themselves from such theft, fraud, or identity theft; and (4) subject to prolonged surreptitious fraud and identity theft following the theft of their data, all of which is well documented in academic and government-issued materials, by experts in the field, and by the media.

142. Through its Privacy Policy and other actions and representations, Zynga held itself out to I.C. and the Nationwide Minor Subclass as possessing and maintaining adequate data security measures and systems that were sufficient to protect the PII belonging to I.C. and the Nationwide Minor Subclass.

143. Zynga owed a heightened duty to I.C. and Nationwide Minor Subclass to communicate accurate information about its compliance with the representations made in its Privacy Policy and about any material weaknesses in its data security systems and procedures.

144. Zynga knew or should have known that it was not in compliance with the representations made in its Privacy Policy.

145. Zynga knowingly and deliberately failed to disclose material weaknesses in its data security systems and procedures that good faith and common decency required it to disclose to I.C. and the Nationwide Minor Subclass.

146. Neither I.C. nor the Nationwide Minor Subclass could have known or discovered the material weaknesses in Zynga's data security practices.

147. A reasonable business would have disclosed information concerning material weaknesses in its data security measures and systems to I.C. and the Nationwide Minor Subclass.

148. Zynga also breached its heightened duty to I.C. and Nationwide Minor Subclass when it failed to properly communicate information concerning the data breach that it knew, or should have known, compromised PII of I.C. and the Nationwide Minor Subclass.

149. I.C. and the Nationwide Minor Subclass justifiably relied on Zynga's representations, or lack thereof, when they provided their PII to Zynga.

150. As a direct and proximate result of Zynga's negligent misrepresentations by omission, I.C. and the Nationwide Minor Subclass have suffered injury, have been damaged as described herein, and are entitled to damages in an amount to be proven at trial.

151. As child victims, I.C. and the Nationwide Minor Subclass have suffered greater harm from Zynga's negligent misrepresentation than adult victims and are thus entitled to increased damages.

COUNT V – Negligence Per Se – FTC Act
(On behalf of Plaintiffs, the Nationwide Class, the Nationwide Adult Subclass, and the Nationwide Minor Subclass)

152. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

153. This count is brought on behalf of all Class members.

154. 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 FTC, the unfair act or practice by companies such as Zynga of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Zynga's duty.

155. Zynga violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII; by failing to comply with applicable industry standards; by falsely representing to its users and the public the nature and scope of the data breach and the need for password resets; and by unduly delaying reasonable notice of the actual breach. Zynga's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, the foreseeable consequences of a data breach, and the foreseeable consequences of misleading its users and the public.

156. Zynga's violation of Section 5 of the FTC Act constitutes negligence per se.

157. Plaintiffs and the Class are within the category of persons the FTC Act was intended to protect.

158. The harm that occurred as a result of the data breach described herein and in the various media reports is the type of harm the FTC Act was intended to guard against.

159. As a direct and proximate result of Zynga's negligence per se, Plaintiffs and the Class have suffered injury, have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Zynga's possession, and are entitled to damages in an amount to be proven at trial.

COUNT VI – Negligence Per Se – FTC Act
(On behalf of I.C. and the Nationwide Minor Subclass)

160. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

161. This count is brought on behalf of I.C. and the Nationwide Minor Subclass.

162. I.C. and the Nationwide Minor Subclass are one of Zynga's principal targeted demographics and account for a sizeable portion of Zynga's total user base, and Zynga has long been aware of that fact.

163. I.C. and the Nationwide Minor Subclass are a particularly vulnerable and defenseless group of Zynga users and are more significantly damaged and imminently threatened to be damaged as a result of Zynga's negligence per se described herein because, without limitation, they are especially: (1) attractive targets to cyber criminals; (2) vulnerable to fraudulent activity and identity theft with respect to their stolen PII; (3) defenseless to protect

themselves from such theft, fraud, or identity theft; and (4) subject to prolonged surreptitious fraud and identity theft following the theft of their data, all of which is well documented in academic and government-issued materials, by experts in the field, and by the media.

164. 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 FTC, the unfair act or practice by companies such as Zynga of failing to use reasonable measures to protect minors' PII. Various FTC publications and orders also form the basis of Zynga's duty.

165. Zynga violated Section 5 of the FTC Act by failing to use reasonable measures to protect minors' PII; by failing to comply with applicable industry standards for protecting minors' PII; by falsely representing to its users and the public the nature and scope of the data breach and the need for password resets; and by unduly delaying reasonable notice of the actual breach. Zynga's conduct was particularly unreasonable given the vulnerability of the child victims, the nature and amount of PII it obtained and stored, the foreseeable consequences of a data breach, and the foreseeable consequences of misleading its users and the public.

166. Zynga's violation of Section 5 of the FTC Act constitutes negligence per se.

167. I.C. and the Nationwide Minor Subclass are within the category of persons the FTC Act was intended to protect.

168. The harm that occurred as a result of the data breach described herein and in the various media reports is the type of harm the FTC Act was intended to guard against.

169. As a direct and proximate result of Zynga's negligence per se, I.C. and the Nationwide Minor Subclass have suffered injury, have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Zynga's possession, and are entitled to damages in an amount to be proven at trial.

170. As child victims, I.C. and the Nationwide Minor Subclass have suffered greater harm from Zynga's negligent misrepresentation than adult victims and are thus entitled to increased damages.

///

///

COUNT VII – Unjust Enrichment
(On behalf of Plaintiffs, the Nationwide Class, the Nationwide Adult Subclass, and the Nationwide Minor Subclass)

171. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

172. This count is brought on behalf of all Class members.

173. Plaintiffs and the Class have an interest, both equitable and legal, in their PII that was collected and maintained by Zynga. This PII was conferred on Zynga directly by Plaintiffs and the Class themselves.

174. Zynga was benefitted by the conferral upon it of the PII pertaining to Plaintiffs and the Class and by its ability to retain and use that information. Zynga understood that it was in fact so benefitted.

175. Zynga also understood and appreciated that the PII pertaining to Plaintiffs and the Class was private and confidential, and its value depended upon Zynga maintaining the privacy and confidentiality of that PII.

176. But for Zynga's willingness and commitment to maintain its privacy and confidentiality, Plaintiffs and the Class would not have transferred PII to Zynga or entrusted their PII to Zynga, and Zynga would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining customers and users of its platform, gaining the reputational advantages conferred upon it by Plaintiffs and the Class, collecting excessive advertising and sales revenues as described herein, monetary savings resulting from failure to reasonably upgrade and maintain DT infrastructures, staffing and expertise raising investment capital as described herein, and realizing excessive profits.

177. As a result of Zynga's wrongful conduct as alleged in this Complaint (including, among other things, its deception of Plaintiffs, the Class, its users in general, and the public relating to the nature and scope of the data breach; its utter failure to employ adequate data security measures; its continued maintenance and use of the PII belonging to Plaintiffs and the Class without having adequate data security measures; and its other conduct facilitating the theft of that PII) Zynga has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs

and the Class.

178. Zynga's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class members' sensitive PII, while at the same time failing to maintain that information secure from intrusion.

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

180. The benefit conferred upon, received, and enjoyed by Zynga was not conferred officiously or gratuitously, and it would be inequitable and unjust for Zynga to retain the benefit.

181. Zynga is therefore liable to Plaintiffs and the Class for restitution in the amount of the benefit conferred on Zynga as a result of its wrongful conduct, including specifically the value to Zynga of the PII that was stolen in the Zynga data breach and the profits Zynga is receiving from the use and sale of that information.

COUNT VIII – Unjust Enrichment
(On behalf of I.C. and the Nationwide Minor Subclass)

182. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

183. This count is brought on behalf of I.C. and the Nationwide Minor Subclass.

184. I.C. and the Nationwide Minor Subclass are one of Zynga's principal targeted demographics and account for a sizeable portion of Zynga's total user base, and Zynga has long been aware of that fact.

185. I.C. and the Nationwide Minor Subclass are a particularly vulnerable and defenseless group of Zynga users and are more significantly damaged and imminently threatened to be damaged as a result of Zynga's unjust enrichment described herein because, without limitation, they are especially: (1) attractive targets to cyber criminals; (2) vulnerable to fraudulent activity and identity theft with respect to their stolen PII; (3) defenseless to protect themselves from such theft, fraud, or identity theft; and (4) subject to prolonged surreptitious

fraud and identity theft following the theft of their data, all of which is well documented in academic and government-issued materials, by experts in the field, and by the media.

186. I.C. and the Nationwide Minor Subclass have an interest, both equitable and legal, in their PII that was collected and maintained by Zynga. This PII was conferred on Zynga directly by I.C. and the Nationwide Minor Subclass themselves.

187. Zynga was benefitted by the conferral upon it of the PII pertaining to I.C. and the Nationwide Minor Subclass and by its ability to retain and use that information. Zynga understood that it was in fact so benefitted.

188. Zynga also understood and appreciated that the PII pertaining to I.C. and the Nationwide Minor Subclass was private and confidential, and its value depended upon Zynga maintaining the privacy and confidentiality of that PII.

189. But for Zynga's willingness and commitment to maintain its privacy and confidentiality, I.C. and the Nationwide Minor Subclass would not have transferred PII to Zynga or entrusted their PII to Zynga, and Zynga would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining customers and users of its platform, gaining the reputational advantages conferred upon it by I.C. and the Nationwide Minor Subclass, collecting excessive advertising and sales revenues as described herein, monetary savings resulting from failure to reasonably upgrade and maintain DT infrastructures, staffing and expertise raising investment capital as described herein, and realizing excessive profits.

190. As a result of Zynga's wrongful conduct as alleged in this Complaint (including, among other things, its deception of I.C., the Nationwide Minor Subclass, its users in general, and the public relating to the nature and scope of the data breach; its utter failure to employ adequate data security measures; its continued maintenance and use of the PII belonging to I.C. and the Nationwide Minor Subclass without having adequate data security measures; and its other conduct facilitating the theft of that PII) Zynga has been unjustly enriched at the expense of, and to the detriment of, I.C. and the Nationwide Minor Subclass.

191. Zynga's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of I.C. and the Nationwide Minor Subclass members' sensitive PII, while at the same time failing to maintain that information secure from intrusion.

192. Under the common law doctrine of unjust enrichment, it is inequitable for Zynga to be permitted to retain the benefits it received, and is still receiving, without justification, from I.C. and the Nationwide Minor Subclass in an unfair and unconscionable manner. Zynga's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

193. The benefit conferred upon, received, and enjoyed by Zynga was not conferred officiously or gratuitously, and it would be inequitable and unjust for Zynga to retain the benefit.

194. Zynga is therefore liable to I.C. and the Nationwide Minor Subclass for restitution in the amount of the benefit conferred on Zynga as a result of its wrongful conduct, including specifically the value to Zynga of the PII that was stolen in the Zynga data breach and the profits Zynga is receiving from the use and sale of that information.

195. As child victims, I.C. and the Nationwide Minor Subclass conferred a greater benefit on Zynga and suffered greater harm from Zynga's wrongful conduct than adult victims, and as a result, I.C. and the Nationwide Minor Subclass are entitled to increased damages.

COUNT IX – Violation of State Data Breach Statutes
(On behalf of all members of the Nationwide Class, the Nationwide Adult Subclass, and the Nationwide Minor Subclass residing in states with applicable data breach statutes)

196. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

197. This count is brought on behalf of all Class members residing in states with applicable data breach statutes.

198. Zynga is in possession of PII belonging to Plaintiffs and the Class and is responsible for reasonably safeguarding that PII consistent with the requirements of the applicable laws pertaining hereto.

199. Despite having the email addresses for the individuals whose PII was stolen, Zynga did not provide notification of the breach to the individuals whose PII was stolen.

200. As to applicable state laws, Zynga failed to safeguard, maintain, and dispose of, as required, the PII within its possession, custody, or control as discussed herein, which it was required to do by the laws of the State of California, Illinois, New Jersey, North Carolina, and all other applicable State laws.

201. Zynga further failed to provide reasonable and timely notice of the data breach to Plaintiffs and the Class as required by the various state data breach notification statutes, including, without limitation, Cal. Civ. Code § 1798.80 *et seq.*; 815 Ill. Comp. Stat. 530/5 *et seq.*; N.J. Stat. § 56:8-163; N.C. Gen. Stat. § 75-61; and other similar state data breach statutes.

202. As a result of Zynga's failure to reasonably safeguard the PII belonging to Plaintiffs and the Class, and Zynga's failure to provide reasonable and timely notice of the data breach to Plaintiffs and the Class, Plaintiffs and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Zynga's possession, and are entitled to damages in an amount to be proven at trial.

COUNT X – Violation of State Data Breach Statutes
(On behalf of I.C. and the Nationwide Minor Subclass)

203. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

204. This count is brought on behalf of I.C. and the Nationwide Minor Subclass members residing in states with applicable data breach statutes.

205. I.C. and the Nationwide Minor Subclass are one of Zynga's principal targeted demographics and account for a sizeable portion of Zynga's total user base, and Zynga has long been aware of that fact.

206. I.C. and the Nationwide Minor Subclass are a particularly vulnerable and defenseless group of Zynga users and are more significantly damaged and imminently threatened to be damaged as a result of Zynga's violation of state data breach statutes described herein because, without limitation, they are especially: (1) attractive targets to cyber criminals; (2) vulnerable to fraudulent activity and identity theft with respect to their stolen PII; (3) defenseless to protect themselves from such theft, fraud, or identity theft; and (4) subject to prolonged surreptitious fraud and identity theft following the theft of their data, all of which is well

documented in academic and government-issued materials, by experts in the field, and by the media.

207. Zynga is in possession of PII belonging to I.C. and the Nationwide Minor Subclass and is responsible for reasonably safeguarding that PII consistent with the requirements of the applicable laws pertaining hereto.

208. Despite having the email addresses for the individuals whose PII was stolen, Zynga did not provide notification of the breach to the individuals whose PII was stolen.

209. As to applicable state laws, Zynga failed to safeguard, maintain, and dispose of, as required, the PII within its possession, custody, or control as discussed herein, which it was required to do by the laws of the State of California, Illinois, New Jersey, North Carolina, and all other applicable State laws.

210. Zynga further failed to provide reasonable and timely notice of the data breach to I.C. and the Nationwide Minor Subclass as required by the various state data breach notification statutes, including, without limitation, Cal. Civ. Code § 1798.80 *et seq.*; 815 Ill. Comp. Stat. 530/5 *et seq.*; N.J. Stat. § 56:8-163; N.C. Gen. Stat. § 75-61; and other similar state data breach statutes.

211. As a result of Zynga's failure to reasonably safeguard the PII belonging to I.C. and the Nationwide Minor Subclass, and Zynga's failure to provide reasonable and timely notice of the data breach to I.C. and the Nationwide Minor Subclass, I.C. and the Nationwide Minor Subclass have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Zynga's possession, and are entitled to damages in an amount to be proven at trial.

212. As child victims, I.C. and the Nationwide Minor Subclass have suffered greater harm from Zynga's violation of state data breach statutes than adult victims and are thus entitled to increased damages.

COUNT XI – Intrusion Upon Seclusion
(On behalf of Plaintiffs and all members of the Nationwide Class, the Nationwide Adult Subclass, and the Nationwide Minor Subclass who reside in Intrusion Upon Seclusion States)

213. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

214. Plaintiffs bring this claim on behalf of persons who reside in: Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont, Washington, West Virginia; and any other state that recognizes a claim for intrusion upon seclusion under the facts and circumstances alleged above (the "Intrusion Upon Seclusion States").

215. Plaintiffs had a reasonable expectation of privacy in the PII that Zynga mishandled.

216. By failing to keep Plaintiffs' Private Information safe, and by misusing and/or disclosing said information to unauthorized parties for unauthorized use, Zynga invaded Plaintiffs' privacy by:

- Intruding into Plaintiffs' private affairs in a manner that would be highly offensive to a reasonable person; and
- Publicizing private facts about the Plaintiffs, which is highly offensive to a reasonable person.

217. Zynga knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' position would consider Zynga's actions highly offensive.

218. Zynga invaded Plaintiffs' right to privacy and intruded into Plaintiffs' private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

219. As a proximate result of such misuse and disclosures, Plaintiffs' reasonable expectation of privacy in their Private Information was unduly frustrated and thwarted. Zynga's conduct amounted to a serious invasion of Plaintiffs' protected privacy interests.

220. In failing to protect Plaintiffs' Private Information, and in misusing and/or disclosing their Private Information, Zynga has acted with malice and oppression and in conscious disregard of Plaintiffs' and the Class Members' rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing its own economic, corporate, and legal interests above the privacy interests of its many millions of users. The

Plaintiffs, therefore, seek an award of damages, including punitive damages, on behalf of Plaintiffs and the Class.

COUNT XII – Intrusion Upon Seclusion
(On behalf of I.C. and the Nationwide Minor Subclass who reside in Intrusion Upon Seclusion States)

221. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

222. I.C. and the Nationwide Minor Subclass bring this claim on behalf of minors who reside in: Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont, Washington, West Virginia, and any other state that recognizes a claim for intrusion upon seclusion under the facts and circumstances alleged above (the "Intrusion Upon Seclusion States").

223. I.C. and the Nationwide Minor Subclass are one of Zynga's principal targeted demographics and account for a sizeable portion of Zynga's total user base, and Zynga has long been aware of that fact.

224. I.C. and the Nationwide Minor Subclass are a particularly vulnerable and defenseless group of Zynga users and are more significantly damaged and imminently threatened to be damaged as a result of Zynga's intrusion upon seclusion described herein because, without limitation, they are especially: (1) attractive targets to cyber criminals; (2) vulnerable to fraudulent activity and identity theft with respect to their stolen PII; (3) defenseless to protect themselves from such theft, fraud, or identity theft; and (4) subject to prolonged surreptitious fraud and identity theft following the theft of their data, all of which is well documented in academic and government-issued materials, by experts in the field, and by the media.

225. I.C. and the Nationwide Minor Subclass had a reasonable expectation of privacy in the PII that Zynga mishandled.

226. By failing to keep I.C.'s and the Nationwide Minor Subclass's Private Information safe, and by misusing and/or disclosing said information to unauthorized parties for unauthorized use, Zynga invaded I.C.'s and the Nationwide Minor Subclass's privacy by:

- Intruding into I.C.'s and the Nationwide Minor Subclass's private affairs in a manner that would be highly offensive to a reasonable person; and
- Publicizing private facts about I.C. and the Nationwide Minor Subclass, which is highly offensive to a reasonable person.

227. Zynga knew, or acted with reckless disregard of the fact that, a reasonable person in I.C.'s and the Nationwide Minor Subclass's position would consider Zynga's actions highly offensive.

228. Zynga invaded I.C.'s and the Nationwide Minor Subclass's right to privacy and intruded into their private affairs by misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

229. As a proximate result of such misuse and disclosures, I.C.'s and the Nationwide Minor Subclass's reasonable expectation of privacy in their Private Information was unduly frustrated and thwarted. Zynga's conduct amounted to a serious invasion of I.C.'s and the Nationwide Minor Subclass's protected privacy interests.

230. In failing to protect I.C.'s and the Nationwide Minor Subclass's Private Information, and in misusing and/or disclosing their Private Information, Zynga has acted with malice and oppression and in conscious disregard of I.C.'s and the Nationwide Minor Subclass's rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing its own economic, corporate, and legal interests above the privacy interests of its many millions of users. I.C. and the Nationwide Minor Subclass, therefore, seek an award of damages, including punitive damages.

231. As child victims, I.C. and the Nationwide Minor Subclass have suffered greater harm from Zynga's privacy intrusion than adult victims and are thus entitled to increased damages, including punitive damages.

COUNT XIII– Declaratory Judgment
(On behalf of Plaintiffs, the Nationwide Class, the Nationwide Adult Subclass, and the Nationwide Minor Subclass)

232. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

233. This count is brought on behalf of all Class members.

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

235. An actual controversy has arisen in the wake of the Zynga data breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' PII and whether Zynga is currently maintaining data security measures adequate to protect Plaintiffs and the Class from further data breaches that compromise their PII. Plaintiffs allege that Zynga's data security measures remain inadequate.

236. Plaintiffs and the Class continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

237. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Zynga continues to owe a legal duty to secure consumers' PII and to timely notify consumers of any data breach and that Zynga is required to establish and implement data security measures that are adequate to secure consumers' PII.

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

239. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury, and Plaintiffs and the Class lack an adequate legal remedy. The threat of another Zynga data breach is real, imminent, and substantial. If another breach at Zynga occurs, Plaintiffs will not have an adequate remedy at law, because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

240. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Zynga if an injunction is issued. Among other things, if another massive data breach occurs at Zynga, Plaintiffs will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to Zynga of complying with an injunction by employing reasonable

prospective data security measures is relatively minimal, and Zynga has a pre-existing legal obligation to employ such measures.

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

COUNT XIV– Declaratory Judgment
(On behalf of I.C. and the Nationwide Minor Subclass)

242. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

243. This count is brought on behalf of I.C. and the Nationwide Minor Subclass.

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

245. An actual controversy has arisen in the wake of the Zynga data breach regarding its present and prospective common law and other duties to reasonably safeguard its minor customers' PII and whether Zynga is currently maintaining data security measures adequate to protect I.C. and the Nationwide Minor Subclass from further data breaches that compromise their PII. I.C. and the Nationwide Minor Subclass allege that Zynga's data security measures remain inadequate to protect the PII of minors.

246. I.C. and the Nationwide Minor Subclass continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

247. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Zynga continues to owe a legal duty to secure minor consumers' PII and to timely notify minor consumers of any data breach and that Zynga is required to establish and implement data security measures that are adequate to secure minor consumers' PII.

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

249. If an injunction is not issued, I.C. and the Nationwide Minor Subclass will suffer irreparable injury, and I.C. and the Nationwide Minor Subclass lack an adequate legal remedy. The threat of another Zynga data breach is real, imminent, and substantial. If another breach at Zynga occurs, I.C. and the Nationwide Minor Subclass will not have an adequate remedy at law, because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

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

251. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Zynga, thus eliminating the additional injuries that would result to I.C. and the Nationwide Minor Subclass and the millions of minor consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of members of the Class, as applicable, respectfully request that the Court enter judgment in their favor and against Zynga, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Counsel as Class Counsel;

2. That Plaintiffs be granted the declaratory relief sought herein;

3. That the Court grant permanent injunctive relief to prohibit Zynga from continuing to engage in the unlawful acts, omissions, and practices described herein;

4. That the Court award Plaintiffs and Class and Class members all statutory damages, including but not limited to compensatory, consequential, and general damages in an amount to be determined at trial;

5. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

6. That the Court award to Plaintiffs all costs and expenses of the action, including reasonable attorneys' fees;

7. That the Court award pre- and post-judgment interest at the maximum legal rate; and

8. That the Court grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution.

9. That the Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all claims so triable.

DESIGNATION OF PLACE OF TRIAL

Plaintiffs hereby designate San Francisco, California as the place of trial for this matter.

Dated: March 2, 2020

By: */s/ Adam J. Zapala*

Adam J. Zapala (SBN 245748)
Reid Gaa (SBN 330141)
COTCHETT, PITRE & McCARTHY, LLP.
840 Malcolm Road, Suite 200
Burlingame, CA 94010
Tel: (650) 697-6000
Fax: (650) 697-0577
azapala@cpmlegal.com
rgaa@cpmlegal.com

THE MILLER LAW FIRM, P.C.
E. Powell Miller (*pro hac vice pending*)
Sharon S. Almonrode (*pro hac vice pending*)

Emily E. Hughes (*pro hac vice pending*)
Dennis A. Lienhardt (*pro hac vice pending*)
William Kalas (*pro hac vice pending*)
950 W. University Dr., Suite 300
Rochester, Michigan 48307
Telephone: (248) 841-2200
Fax: (248) 652-2852
epm@millerlawpc.com
ssa@millerlawpc.com
eeh@millerlawpc.com
dal@millerlawpc.com
wk@millerlawpc.com

FOULSTON SIEFKIN LLP

Scott C. Nehrbass (*pro hac vice pending*)
Daniel J. Buller (*pro hac vice pending*)
32 Corporate Woods, Suite 600
9225 Indian Creek Parkway
Overland Park, KS 66210-2000
(913) 253-2144
(866) 347-1472 FAX
snehrbass@foulston.com
dbuller@foulston.com

~and~

Boyd A. Byers (*pro hac vice pending*)
Jeremy E. Koehler (*pro hac vice pending*)
Foulston Siefkin LLP
1551 N. Waterfront Parkway, Suite 100
Wichita, Kansas 67206-4466
Tel. (Direct): 316-291-9796
Fax: 866-559-6541
bbyers@foulston.com
jkoehler@foulston.com

Counsel for Plaintiffs I.C., Amy Gitre, and the Putative Class