Hassan A. Zavareei (State Bar No. 181547)
Mark Clifford*
TYCKO & ZAVAREEI LLP
1828 L Street NW, Suite 1000
Washington, D.C. 20036
Telephone: (202) 973-0900
Facsimile: (202) 973-0950
hzavareei@tzlegal.com
mclifford@tzlegal.com

Counsel for Plaintiffs and the Proposed Classes
**Pro Hac Vice Forthcoming*
(Additional Counsel on Signature Page)

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

CAROL JOHNSON and LISA THOMAS,

On Behalf of Themselves and All Others Similarly Situated,

Plaintiff,

v.

ZYNGA, INC.,

Defendant.

CLASS ACTION COMPLAINT FOR DAMAGES, EQUITABLE, INJUNCTIVE, and DECLARATORY RELIEF

DEMAND FOR JURY TRIAL

Plaintiffs Carol Johnson ("Ms. Johnson") and Lisa Thomas ("Ms. Thomas") (collectively, "Plaintiffs") , individually and on behalf of all other persons similarly situated, and through their attorneys of record, alleges the following against Defendant Zynga, Inc. ("Defendant" or "Zynga") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

INTRODUCTION

1. On September 12, 2019, Zynga updated its website to post a "Player Security Announcement," which stated that "certain player account information may have been illegally accessed by outside hackers."[1] This unauthorized access is referred to herein as the "Zynga Data Breach." Zynga has not to date sent any email or other form of communication to its users informing them of the Zynga Data Breach.

2. A hacker that goes by the alias Gnosticplayers accessed Zynga's computer systems and stole information associated with 173 million user accounts.[2] The Zynga Data Breach included the following personally identifiable information ("PII"): names, email addresses, login ids, passwords, password reset tokens, phone numbers, Facebook IDs, and Zynga account IDs.[3]

3. Although Zynga claims that "we do not believe any financial information was accessed," it noted that "the investigation is ongoing."[4] Zynga has provided no update, and thus Plaintiffs do not know if financial information associated with their accounts was stolen in the Zynga Data Breach.

4. Plaintiffs and the Classes, as defined herein, had their PII stolen as a result of the Zynga Data Breach and suffered harm directly as a result of the Zynga Data Breach.

---

[1] https://investor.zynga.com/news-releases/news-release-details/player-security-announcement

[2] Gary Guthrie, *Words With Friends and other Zynga game players may have had their data hacked*, Consumer Affairs (Dec. 26, 2019), https://www.consumeraffairs.com/news/words-with-friends-and-other-zynga-game-players-may-have-had-their-data-hacked-122619.html

[3] Swati Khandelwal, *Exclusive – Hacker Steals over 218 Million Zynga 'Words with Friends' Gamers Data*, Hacker News (Sep. 29, 2019), https://thehackernews.com/2019/09/zynga-game-hacking.html.

[4] https://investor.zynga.com/news-releases/news-release-details/player-security-announcement

PARTIES

5. Ms. Johnson is a citizen of the state of Missouri, and at all relevant times has resided in Rogersville, Missouri, and has provided PII to Zynga in the process of creating an account for accessing and playing Zynga games. Ms. Johnson's PII was stolen in the Zynga Data Breach.

6. Ms. Thomas is a citizen of the state of Wisconsin, and currently and at the time of the Zynga Data Breach resided in Manitowoc, Wisconsin, and has provided PII to Zynga in the process of creating an account for accessing and playing Zynga games. Ms. Thomas' PII was stolen in the Zynga Data Breach.

7. Defendant Zynga, Inc. is a corporation incorporated in the State of Delaware with its headquarters and principle place of business in San Francisco, California.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members are citizens of a different state than Defendant.

9. This Court has personal jurisdiction over Defendant Zynga because it has its headquarters in and principal place of business in San Francisco, California and regularly transacts business in the state of California.

10. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because Zynga's headquarters and principal place of business are located in this District, Zynga resides in this District, and substantial parts of the events or omissions giving rise to the claims occurred in or emanated from this District, including, without limitation, decisions made by Zynga's governance and management personnel or inaction by those individuals that led to misrepresentations, invasions of privacy, and the Zynga Data Breach.

FACTUAL ALLEGATIONS

Zynga's Collection of Users' PII

11. Zynga is a video game developer and refers to 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."[5] Zynga's games include the popular "Words With Friends" game, Words With Friends 2, Draw Something, Farmville, and Zynga Poker, among other games.[6] In the third quarter of 2019, Zynga had as many as 67 million monthly active users.[7]

12. Zynga offers a mix of paid and "free" games, which are available for download from common mobile application stores, such as the iTunes Store or Google Play. Zynga is able to offer "free" games by supporting those games with advertisements, in-game purchases, and the collection of its users' PII.

13. Whenever a consumer wishes to download and play a Zynga game, such as Words With Friends, the consumer must create a Zynga user account. The consumer must provide their first name, last name, email address, and gender, and must create a password to accompany the account. Users may link their Zynga account to their Facebook account instead of providing an email address (which requires providing Zynga with the consumer's Facebook username and password). Zynga does not, as of the date of this Complaint, collect information that would disclose a user's age, such as date of birth.

14. Zynga retains in its databases its users' names, email addresses, login IDs, passwords, password reset tokens, phone numbers, Facebook IDs, and Zynga account IDs. When financial information is provided, such as for in-app purchases, Zynga retains this information as well.

15. The PII provided to Zynga is governed by its Privacy Policy, which provides detailed information about what types of PII will be shared and with what entities. It further promises to

---

[5] Zynga Homepage, https://www.zynga.com/ (last visited March 23, 2020)
[6] *Games*, Zynga, https://www.zynga.com/games/ (last visited March 23, 2020)
[7] *Average monthly active users (MAU) of Zynga games from 4th quarter 2012 to 3rd quarter 2019*, Statista, https://www.statista.com/statistics/273569/monthly-active-users-of-zynga-games/ (last visited March 13, 2020).

"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."[8]

16. Ms. Johnson created a Zynga user account in 2016 in order to play the popular Words With Friends game. In doing so, she provided the PII described above to Zynga.

17. Ms. Thomas created a Zynga user account in or about 2014 in order to play the popular Words With Friends and Draw Something games. In doing so, she provided the PII described above to Zynga. Ms. Thomas also made at least one "in-app" purchase from Zynga, paid for with a debit card linked to her Google Play account.

18. Plaintiffs provided their PII to Zynga with the expectation and understanding that Zynga would adequately protect and store their data. If they had known that Zynga's data security was insufficient to protect their PII, they would not have entrusted their PII to Zynga, created a Zynga user account, downloaded Zynga games, and would not have been willing to pay for, or pay as much for, any game purchase (either purchasing gaming apps or making in-app purchases).

Zynga's Underage Customers

19. Although Zynga does not collect information that would disclose the age of its users, upon information and belief, a significant portion of Zynga's users are children. Approximately 8% of mobile gamers are children aged 13 to 17.[9]

20. Many of Zynga's games are plainly targeted to children, with colorful graphics and easy-to-use interfaces.

21. Zynga has disclosed in its securities filings that it must comply with regulations governing "the collection of data from minors."[10] Zynga also acknowledges the "increased attention being given to

---

[8] *Privacy Policy*, Zynga (Sep. 9, 2019), https://web.archive.org/web/20190909053717/https://www.zynga.com/privacy/policy

[9] *The Mobile Gaming Industry: Statistics, Revenue, Demographics, More [Infographic]*, Mediakix, https://mediakix.com/blog/mobile-gaming-industry-statistics-market-revenue/ (last visited March 13, 2020)

[10] *See, e.g.*, Form 10-K For the Fiscal Year Ended December 31, 2019, Zynga, Inc, https://www.sec.gov/Archives/edgar/data/1439404/000156459020007803/znga-10k_20191231.htm (last visited March 13, 2020).

the collection of data from minors" and that it "devote[s] significant operational resources and incur[s] significant expenses" in its effort to comply with data privacy laws, including those specific to minors.[11]

22. And Zynga's founder and Executive Chairman even acknowledged the addictiveness of mobile games for children during an April 2013 interview with the New York Times, when he was still the company's CEO.[12]

The Zynga Data Breach

23. In September 2019, hacker Gnosticplayers bragged to the website *The Hacker News* that he had hacked Zynga, claiming that "he managed to breach 'Words With Friends', a popular Zynga-developed word puzzle game, and unauthorizedly access a massive database of more than 218 million users."[13] Later reports would put the actual number of accounts breached at closer to 173 million.

24. Gnosticplayers also "claims to have hacked data belonging to some other Zynga-developed games, including Draw Something and the discontinued OMGPOP game, which allegedly exposed clear text passwords for more than 7 million users."[14]

25. According to a sample of user data Gnosticplayers provided to *The Hacker News*, the Zynga Data Breach included the following user information: names, email addresses, login ids, passwords, password reset tokens, phone numbers, Facebook IDs, and Zynga account IDs (collectively, the "PII").[15]

26. Gnosticplayers is a prolific hacker, having already sold stolen PII on the dark web on at least five separate occasions, totaling over "one billion user credentials and personal details stolen from roughly 44 companies."[16]

27. Rather than informing users of the Zynga Data Breach by contacting their email addresses that were provided during account creation, or through a pop-up notification in its gaming applications,

---

[11] *Id.* At 13.
[12] Andrew Goldman, *Mark Pincus Thinks Angry Birds Won't Hurt Your Kids*, N.Y. Times (April 5, 2013), https://www.nytimes.com/2013/04/07/magazine/mark-pincus-thinks-angry-birds-wont-hurt-your-kids.html.
[13] Swati Khandelwal, *Exclusive – Hacker Steals over 218 Million Zynga 'Words with Friends' Gamers Data*, Hacker News (Sep. 29, 2019), https://thehackernews.com/2019/09/zynga-game-hacking.html.
[14] *Id.*
[15] *Id.*
[16] Cyware News, *Times when 'Gnosticplayers' hacker made headlines for selling troves of stolen data on dark web*, Cyware Social (Sep. 30, 2019), https://cyware.com/news/times-when-gnosticplayers-hacker-made-headlines-for-selling-troves-of-stolen-data-on-dark-web-f8849502.

Zynga instead simply posted a "Player Security Announcement" to its website on September 12, 2019, which stated that "certain player account information may have been illegally accessed by outside hackers."[17] Zynga has not updated its Player Security Announcement since it was first posted.[18]

28. Many, if not most, Zynga users do not even know that their PII has been accessed. There is no reason for users to access Zynga's website when using Zygna's mobile game applications. They would only know if they checked the Zynga website, noticed instances of fraud or identity theft connected to their PII, or received notice from some third-party website.

29. One such website, named "Have I Been Pwned," which allows users to enter their credentials to determine whether they were victims of a hack and to sign up for notifications of potential hacks, distributed an alert on December 18, 2019 to its subscriber list regarding the Zynga Data Breach.[19]

30. Plaintiffs' PII were stolen in the Zynga Data Breach, as confirmed by checking the "Have I Been Pwned" websit

31. That Plaintiffs' and the class member's PII was accessible in plain text formatting (with the exception of some passwords) establishes that Zynga did not take adequate data security measures to store and protect its users' PII.

32. Moreover, Zynga only stored its users' passwords with "SHA1" encryption. But it was widely known *over two years before* the Zynga Data Breach that SHA1 encryption was inadequate for protecting sensitive information such as passwords.[20]

33. Zynga appreciated and intentionally assumed a known risk that storing PII in unencrypted form, or with a weak SHA1 encryption, would make it a target for hackers. It was these known vulnerabilities that made the Zynga Data Breach so damaging to its victims.

---

[17] https://zyngasupport.helpshift.com/a/zynga/?p=all&l=en&s=announcements&f=player-security-announcement (last visited March 13, 2020).

[18] *Id.* (noting "Last Updated: 174d[ays]").

[19] have i been pwned? Homepage, https://haveibeenpwned.com/ (last visited March 23, 2020).

[20] *See, e.g.*, Lucian Constantin, *The SHA1 hash function is now completely unsafe*, Computerworld (Feb. 23, 2017), https://www.computerworld.com/article/3173616/the-sha1-hash-function-is-now-completely-unsafe.html.

34. At all relevant times, Zynga was well-aware, or reasonably should have been aware, that the PII collected, maintained, and stored on its servers is highly sensitive, susceptible to attack, and could be used for malicious purposes by third parties, such as identity theft, fraud and other misuse.

35. Indeed, in a SEC filing just one month before Zynga notified the public of the Zynga Data Breach, the company acknowledged that "[w]e have experienced and will continue to experience hacking attacks of varying degrees from time to time, including denial-of-service attacks. Because of our prominence in the social game industry, we believe we are a particularly attractive target for hackers."[21]

36. Notwithstanding this knowledge, Zynga did not take adequate security measures to protect Plaintiffs' and class members' PII.

Effect of the Zynga Data Breach on Impacted Customers

37. Zynga's failure to keep Plaintiffs' and class members' PII secure has severe ramifications. Given the sensitive nature of the PII stolen in the Zynga Data Breach—names, email addresses, login ids, passwords, password reset tokens, phone numbers, Facebook IDs, and Zynga account IDs—hackers have the ability to commit identity theft and other identity-related fraud against Plaintiffs and class members now and into the indefinite future.

38. The PII exposed in the Zynga Data Breach is highly coveted and valuable on underground or black markets. For example, a cyber "black market" exists in which criminals openly post and sell stolen consumer information on underground internet websites known as the "dark web"—exposing consumers to identity theft and fraud for years to come.

39. PII has significant monetary value in part because criminals continue their efforts to obtain this data.[22] In other words, if any additional breach of sensitive data did not have incremental value to criminals, one would expect to see a reduction in criminal efforts to obtain such additional data over time. Instead, just the opposite has occurred. For example, the Identity Theft Resource Center reported

---

[21] Form 10-Q For the Quarterly Period Ended June 30, 2019, Zynga, Inc. (filed Aug. 1, 2019) at 49, https://www.sec.gov/Archives/edgar/data/1439404/000156459019028029/0001564590-19-028029-index.htm.

[22] *Data Breaches Rise as Cybercriminals Continue to Outwit IT*, CIO MAGAZINE (Sept. 28, 2014), available at http://www.cio.com/article/2686167/data-breach/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html.

1,473 data breaches in 2019, which represents a 17 percent increase from the total number of breaches reported in 2018.[23]

40. The PII of consumers remains of high value to identity criminals, as evidenced by the prices criminals will pay through black-market sources on the dark web. Numerous sources cite dark web pricing for stolen identity credentials, quantifying the loss to victims based on the value of the data itself. For example, login information for just one social media account can fetch $50 on the dark web.[24]

41. Just as companies like Zynga trade on the value of consumers' PII, consumers recognize the value of their PII and offer it in exchange for goods and services. Plaintiffs gave Zynga their PII in exchange for Zynga's services; namely, access to Words with Friends and Draw Something.

42. Annual monetary losses for victims of identity theft are in the billions of dollars. In 2017, fraudsters stole $16.8 billion from consumers in the United States, which includes $5.1 billion stolen through bank account take-overs.[25]

43. The annual cost of identity theft is even higher. McAfee and the Center for Strategic and International Studies estimates that the likely annual cost to the global economy from cybercrime is $445 billion a year.[26]

44. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, in addition to the irreparable damage that may result from the theft of PII, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found

---

[23] Identity Theft Center, *2019 End-of-Year Data Breach Report* (2019), available at https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf.

[24] *Here's How Much Thieves Make By Selling Your Personal Data Online,* BUSINESS INSIDER (May 27, 2015), available at http://www.businessinsider.com/heres-how-much-your-personal-data-costs-on-the-dark-web-2015-5.

[25] Javelin, *2018 Identity fraud: Fraud Enters A New Era of Complexity*, available at https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity (last visited March 13, 2020).

[26] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited March 13, 2020).

that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[27]

45. And, the impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans or mortgages.[28] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

46. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey[29] evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed
- 67% reported anxiety
- 66% reported feelings of fear related to personal financial safety
- 37% reported fearing for the financial safety of family members
- 24% reported fear for their physical safety
- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft
- 7% reported feeling suicidal.

47. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances
- 37.1% reported an inability to concentrate / lack of focus
- 28.7% reported they were unable to go to work because of physical symptoms

---

[27] U.S. Department of Justice, *Victims of Identity Theft, 2014* (Revised November 13, 2017), available at http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited March 13, 2020).
[28] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, available at https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited March 13, 2020).
[29] *Id.*

- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues)
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[30]

48. There may also be a significant time lag between when PII is stolen and when it is actually misused. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[31]

49. There is a risk of identity theft even where particularly detailed personal information is not stolen, but where the information, such as that which was stolen in the Zynga Data Breach, comprises usernames, email addresses, and passwords.

50. Consumers often reuse passwords. By unlawfully obtaining this information, cyber criminals can use these credentials to access other services beyond that which was hacked.

51. The foregoing problems are compounded where the victims of the Zynga Data Breach are minors.

52. Over 1 million minor children were victims of fraud or identity theft in 2017, and two/thirds of those victims were under the age of seven.[32]

53. Data thieves are also more likely to target minors' PII and to use that PII once it is stolen. In 2017, "[a]mong notified breach victims . . . 39 percent of minors became victims of fraud, versus 19 percent of adults."[33]

---

[30] *Id.*
[31] U.S. Government Accountability Office, *Report to Congressional Requesters* (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited March 13, 2020).
[32] Kelli B. Grant, *Identity Theft isn't just an adult problem. Kids are victims, too*, CNBC (April 24, 2018), https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html.
[33] *Id.*

54. Criminals make use of minors' PII to open accounts or new lines of credit that may not be noticed by the minor; and to create "synthetic identities" using a combination of real and fictitious information which again, the minor may not realize was stolen.[34] Because minors do not regularly monitor their bank accounts (if they have them) or their credit reports, data thieves are more likely to make unrestricted use of this information for longer periods of time than they would for adult victims.[35]

55. Minors also generally are less likely to receive notice from the company responsible for the data breach or to even realize that a thief has made fraudulent use of their information in other ways – such as creating a new identity for the purposes of accessing government benefits, healthcare, or employment.[36] Minors often "won't find out that their identity has been stolen until they apply for their first credit card or college loan."[37]

56. Children are also particularly susceptible to physical harm in the event of a data breach. Data thieves can use their PII "to link a child to his or her parents and pinpoint the child's physical address."[38]

57. Plaintiffs and the Classes (as defined below) would not have provided their account information and other PII to Zynga if they had known Zynga did not have in place adequate policies and procedures to protect their PII, or if they had known that Zynga would effectively keep them in the dark about any breach and theft of their PII.

58. As the result of the Zynga Data Breach, Plaintiffs and class members have suffered or will suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

---

[34] *Id.*

[35] Ron Lieber, *Identity Theft Poses Extra Troubles for Children*, N.Y. Times (April 16, 2015), https://www.nytimes.com/2015/04/18/your-money/a-childs-vulnerability-to-identity-theft.html.

[36] *Id.*

[37] Larry Magid, *Teens Vulnerable to Identity Theft, Financial Crimes, and Impersonation*, Forbes (Nov. 7, 2013), https://www.forbes.com/sites/larrymagid/2013/11/07/teens-concerned-about-identity-theft/#6ab243211c49.

[38] Daniel Victor, *Security Breach at Toy Maker Vtech Includes Data on Children*, N.Y. Times (Nov. 30, 2015), https://www.nytimes.com/2015/12/01/business/security-breach-at-toy-maker-vtech-includes-data-on-children.html.

- purchasing services they would not have otherwise paid for and/or paying more for services than they otherwise would have paid, had they known the truth about Defendant's substandard data security practices;
- losing the inherent value of their PII;
- identity theft and fraud resulting from theft of their PII;
- costs associated with the detection and prevention of identity theft and unauthorized use of their online accounts, including financial accounts;
- costs associated with purchasing credit monitoring and identity theft protection services;
- lowered credit scores resulting from credit inquiries following fraudulent activities;
- costs associated with time spent and the loss of productivity or enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Zynga Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Zynga Data Breach; and
- the continued imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being in the possession of one or more unauthorized third parties.

59. Additionally, Plaintiffs and class members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[39]

---

[39] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 11, 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited March 13, 2020).

60. Consequently, had consumers known the truth about Zynga's data security practices—that Zynga would not adequately protect and store their data—they would not have entrusted their PII to Zynga, created a Zynga user account, downloaded Zynga games, and would not have been willing to pay for, or pay as much for, any game purchase (either purchasing gaming apps or in-app purchase). As such, Plaintiffs and class members did not receive the benefit of their bargain with Zynga because they paid for a value of services, either through PII or a combination of their PII and money, they expected but did not receive.

CLASS ACTION ALLEGATIONS

61. Pursuant to Fed. R. Civ. P. 23(a), (b)(1), (b)(2) and (b)(3), as applicable, Plaintiffs seek certification of the following nationwide class (the "Nationwide Class"):

62. Nationwide Class: **All persons in the United States whose PII was compromised in the Zynga Data Breach.**

63. The Nationwide Class asserts claims against Zynga for negligence (Count 1), negligence *per se* (Count 2), unjust enrichment (Count 3), declaratory judgment (Count 4), breach of confidence (Count 5), breach of contract (Count 6), breach of implied contract (Count 7), and violation of California's Unfair Competition Law (Count 8).

64. Pursuant to Fed. R. Civ. P. 23(a), (b)(2) and (b)(3), as applicable, Ms. Johnson seeks certification of Missouri state claims in the alternative to the nationwide claims, as well as statutory claims under Missouri's consumer protection statute (Count 9) (the "Missouri Subclass"), defined as follows:

65. Missouri Subclass: **All persons in Missouri whose PII was compromised in the Zynga Data Breach.**

66. Pursuant to Fed. R. Civ. P. 23(a), (b)(2) and (b)(3), as applicable, Ms. Thomas seeks certification of Wisconsin state claims in the alternative to the nationwide claims, as well as statutory claims under Wisconsin's consumer protection statute (Count 10) (the "Wisconsin Subclass" and, together with the Missouri Subclass, the "Subclasses"),[40] defined as follows:

[40] The Class and State Subclasses are sometimes referred to herein as "Classes."

67. Wisconsin Subclass: **All persons in Wisconsin whose PII was compromised in the Zynga Data Breach.**

68. Excluded from the Nationwide Class and the Subclasses are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class and the Subclasses are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

69. Plaintiffs reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

70. Each of the proposed classes meets the criteria for certification under Rule 23(a), (b)(1), (b)(2), (b)(3) and (c)(4).

71. As the proposed class members include millions of users across all 50 states, there is significant risk of inconsistent or varying adjudications with respect to individual class members that would establish incompatible standards of conduct for the Defendant. For example, injunctive relief may be entered in multiple cases, but the ordered relief may vary, causing the Defendant to have to chose between differing means of upgrading its data security infrastructure and choosing the court order with which it will comply.

72. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Nationwide Class and the Subclasses are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of class members is unknown to Plaintiffs at this time, public reporting estimates that the PII of approximately 173 million persons was compromised in the Data Breach. Those persons' names and email addresses are available from Zynga's records, and class members may be notified of the pendency of this action by recognized, court-approved notice dissemination methods, which may include electronic mail, U.S. Mail, internet notice, and/or published notice.

73. **Predominance of Common Issues. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions

of law and fact that predominate over any questions affecting individual class members. The common questions include:

a. Whether Defendant knew or should have known that its computer and data storage systems were vulnerable to attack;

- Whether Defendant omitted or misrepresented material facts regarding the security of its computer and data storage systems and its inability to protect the vast amounts of consumer data, including Plaintiffs' and class members' PII;

b. Whether Defendant failed to take adequate and reasonable measures to ensure such computer and data systems were protected;

c. Whether Defendant failed to take available steps to prevent and stop the Zynga Data Breach from happening;

d. Whether Defendant owed duties to Plaintiffs and class members to protect their PII;

e. Whether Defendant owed a duty to provide timely and accurate notice of the Zynga Data Breach to Plaintiffs and class members;

f. Whether Defendant breached its duty to provide timely and accurate notice of the Zynga Data Breach to Plaintiffs and class members;

g. Whether Defendant breached its duties to protect the PII of Plaintiffs and class members by failing to provide adequate data security;

h. Whether Defendant's failure to secure Plaintiffs' and class members' PII in the manner alleged violated federal, state and local laws, or industry standards;

i. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Zynga Data Breach, resulting in the unauthorized access to and/or theft of Plaintiffs' and class members' PII;

j. Whether Defendant has a contractual obligation to use reasonable security measures and whether it complied with such contractual obligation;

k. Whether Defendant's conduct amounted to violations of state consumer protection statutes, and/or state data breach statutes;

l. Whether, as a result of Defendant's conduct, Plaintiffs and class members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled;

m. Whether, as a result of Defendant's conduct, Plaintiffs and class members are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief.

74. **Typicality. Fed. R. Civ. P. 23(a)(3).** As to the Nationwide Class and the Subclasses, Plaintiffs' claims are typical of other class members' claims because Plaintiffs and class members were subjected to the same allegedly unlawful conduct and damaged in the same way.

75. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Nationwide Class and the Missouri and Wisconsin Subclasses because Ms. Johnson and Ms. Thomas are members of the Nationwide Class and the Missouri and Wisconsin Subclasses, respectively, and are committed to pursuing this matter against Defendant to obtain relief for the Classes. Plaintiffs have no conflicts of interest with the Classes. Plaintiffs' counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation and consumer protection claims. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the interests of the Nationwide Class and the Subclasses.

76. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs and class members may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the class members are relatively small compared to the burden and expense required to individually litigate their claims against Defendant, and thus, individual litigation to redress Defendant's wrongful conduct would be impracticable. Individual litigation by each class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

77. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Nationwide Class and the Subclasses as a whole, making injunctive and declaratory relief appropriate to the Classes as a whole. Moreover, Defendant continues to maintain its inadequate security practices, retains possession of Plaintiffs' and the class members' PII, and has not been forced to change its practices or to relinquish PII by nature of other civil suits or government enforcement actions, thus making injunctive and declaratory relief a live issue and appropriate to the Classes as a whole.

78. All members of the proposed Classes are readily ascertainable. Zynga has access to information regarding which individuals were affected by the Zynga Data Breach. Using this information, the members of the Classes can be identified and their contact information ascertained for purposes of providing notice to the Classes.

CLAIMS ON BEHALF OF THE CLASSES

Count 1

NEGLIGENCE

Against Zynga on Behalf of Plaintiffs and the Nationwide Class,

or Alternatively, on behalf of Plaintiffs and the Subclasses

79. Plaintiffs repeat the allegations in paragraphs 1 – 78 in this Complaint, as if fully alleged herein.

80. Zynga required Plaintiffs and class members to submit sensitive PII in order to obtain access to Zynga's online gaming applications. Zynga stored this vast treasure trove of PII on its computer systems.

81. By collecting, storing, using, and profiting from this data, Zynga had a duty of care to Plaintiffs and class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting this PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Defendant's security systems and data storage architecture to ensure that Plaintiffs' and class members' PII was adequately secured and protected; (b) implementing processes that would detect an unauthorized breach of Defendant's security systems and data storage

architecture in a timely manner; (c) timely acting on all warnings and alerts, including public information, regarding Defendant's security vulnerabilities and potential compromise of the compiled data of Plaintiffs and millions of class members; (d) maintaining data security measures consistent with industry standards; and (e) timely and adequately informing class members if and when a data breach occurred notwithstanding undertaking (a) through (d) above.

82. Zynga had common law duties to prevent foreseeable harm to Plaintiffs and class members. These duties existed because Plaintiffs and class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiffs and class members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Defendant knew that it was more likely than not Plaintiffs and other class members would be harmed by such theft.

83. Defendant had a duty to monitor, supervise, control, or otherwise provide oversight to safeguard the PII that was collected and stored on the Zynga's computer systems.

84. Defendant's duties to use reasonable security measures also arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiffs and class members, on the other hand. The special relationship arose because Plaintiffs and class members entrusted Defendant with their PII as part of the creation of user accounts necessary to access Zynga's online and mobile gaming applications. Defendant alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Zynga Data Breach.

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

86. Defendant knew or should have known that its computer systems and data storage architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential PII.

87. Defendant breached the duties it owed to Plaintiffs and class members described above and thus were negligent. Defendant breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiffs and class members; (b) detect the breach while it was ongoing or even promptly after it occurred; and (c) maintain security systems consistent with industry standards.

88. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and class members, their PII would not have been compromised.

89. As a direct and proximate result of Defendant's negligence, Plaintiffs and class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Zynga Data Breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

Count 2

NEGLIGENCE *PER SE*

Against Zynga on Behalf of Plaintiffs and the Nationwide Class,

or Alternatively, on behalf of Plaintiffs and the Subclasses

90. Plaintiffs repeat the allegations in paragraphs 1 – 78 in this Complaint, as if fully alleged herein.

91. Section 5 of the FTC 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 Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

92. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

93. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

94. Plaintiffs and class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

95. Moreover, the harm that has occurred is the type of harm the FTC Act (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 class members.

96. As a direct and proximate result of Defendant's negligence, Plaintiffs and class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Zynga Data Breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

Count 3

UNJUST ENRICHMENT

Against Zynga on Behalf of Plaintiffs and the Nationwide Class,

or Alternatively, on behalf of Plaintiffs and the Subclasses

97. Plaintiffs repeat the allegations in paragraphs 1 – 78 in this Complaint, as if fully alleged herein

98. Plaintiffs and class members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, and maintained by Defendant and that was ultimately stolen in the Zynga Data Breach.

99. Defendant was benefited by the conferral upon it of the PII pertaining to Plaintiffs and class members and by its ability to retain, use, and profit from that information. Defendant understood that it was in fact so benefited.

100. Defendant also understood and appreciated that the PII pertaining to Plaintiffs and class members was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

101. But for Defendant's willingness and commitment to maintain its privacy and confidentiality, that PII would not have been transferred to and entrusted with Defendant.

102. Defendant continues to benefit and profit from its retention and use of the PII while its value to Plaintiffs and class members has been diminished.

103. Defendant also benefitted through its unjust conduct by selling online and mobile gaming applications, or in-app purchases, or by gaining users of its free gaming applications to which it could display paid advertisements, for more than those services were worth to Plaintiffs and class members, who would not have obtained Defendant's online and mobile gaming applications at all, or at the terms offered by Zynga, had they been aware that Defendant would fail to protect their PII.

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

105. It is inequitable for Defendant to retain these benefits.

106. As a result of Defendant's wrongful conduct as alleged in this Complaint (including, among other conduct, its knowing failure to employ adequate data security measures, its continued maintenance and use of the PII belonging to Plaintiffs and class members without having adequate data security measures, and its other conduct facilitating the theft of that PII), Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and class members.

107. Defendant'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' PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

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

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

110. Plaintiffs and the class members have no adequate remedy at law.

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

Count 4

DECLARATORY JUDGMENT

Against Zynga on Behalf of Plaintiffs and the Nationwide Class,

or Alternatively, on behalf of Plaintiffs and the Subclasses

112. Plaintiffs repeat the allegations in paragraphs 1 – 78 in this Complaint, as if fully alleged herein

113. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., the 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.

114. An actual controversy has arisen in the wake of the Zynga Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard its customers' PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and class members from further data breaches that compromise their PII. Plaintiffs and class members remain at imminent risk that further compromises of their PII will occur in the future. This is true even if they are not actively using Defendant's online games or mobile applications.

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

a. Defendant continues to owe a legal duty to secure customers' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

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

116. The Court also should issue corresponding prospective injunctive relief pursuant to 28 U.S.C. §2202, requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumers' PII.

117. If an injunction is not issued, Plaintiffs and class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Zynga. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiffs and class members 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.

118. The hardship to Plaintiffs and class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at Zynga, Plaintiffs and class members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

119. 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 additional injuries that would result to Plaintiff, class members, and the millions of consumers whose PII would be further compromised.

Count 5

BREACH OF CONFIDENCE

Against Zynga on Behalf of Plaintiffs and the Nationwide Class,

or Alternatively, on behalf of Plaintiffs and the Subclasses

120. Plaintiffs repeats the allegations in paragraphs 1 – 78 in this Complaint, as if fully alleged herein.

121. At all times during Plaintiffs' and class members' interactions with Zynga, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and class members' PII.

122. As alleged herein and above, Zynga's relationship with Plaintiffs and class members was governed by terms and expectations that Plaintiffs' and class members' protected PII would be collected, stored, and protected in confidence, and would not be disclosed to the public or any unauthorized third parties.

123. Plaintiffs' and class members provided their respective PII to Zynga with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to the public or any unauthorized parties.

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

125. Zynga voluntarily received in confidence Plaintiffs' and class members' PII with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

126. Due to Zynga's failure to prevent, detect, avoid the Zynga Data Breach from occurring by following best information security practices to secure Plaintiffs' and class members' PII, Plaintiffs'

and class members' PII was disclosed and misappropriated to the public and unauthorized third parties beyond Plaintiffs' and class members' confidence, and without their express permission.

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

128. The injury and harm Plaintiffs and class members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and class members' PII. Zynga knew its computer systems and technologies for accepting, securing, and storing Plaintiffs' and class members' PII had serious security vulnerabilities because Zynga failed to observe even basic information security practices or correct known security vulnerabilities.

129. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Zynga Data Breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

Count 6

BREACH OF CONTRACT

Against Zynga on Behalf of Plaintiffs and the Nationwide Class,

or Alternatively, on behalf of Plaintiffs and the Subclasses

130. Plaintiffs repeats the allegations in paragraphs 1 – 78 in this Complaint, as if fully alleged herein.

131. Zynga's Privacy Policy (the "Privacy Policy") is an agreement between Zynga and persons who provide their PII to Zynga, including Plaintiffs and the class members.

132. The Privacy Policy, as it was in effect at the time of the Zynga Data Breach, states 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.

133. The Privacy Policy provides detailed information about what types of PII will be shared and with what entities. It further promises 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."

134. 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.

135. Plaintiffs and class members fully performed their obligations under the contract with Zynga.

136. 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.

137. 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 that they did not get the benefit of the bargain pursuant to which they provided their PII to Zynga.

Count 7

BREACH OF IMPLIED CONTRACT

Against Zynga on Behalf of Plaintiffs and the Nationwide Class,

or Alternatively, on behalf of Plaintiffs and the Subclasses

138. Plaintiffs repeat the allegations in paragraphs 1 – 78 in this Complaint, as if fully alleged herein, and assert this claim in the alternative to their breach of contract claim to the extent necessary.

139. Plaintiffs and class members also entered into an implied contract with Zynga when they obtained services from Zynga, or otherwise provided PII to Zynga.

140. As part of these transactions, Zynga agreed to safeguard and protect the PII of Plaintiffs and the class members.

141. Plaintiffs and class members entered into implied contracts with the reasonable expectation that Zynga's data security practices and policies were reasonable and consistent with industry standards. Plaintiffs and class members believed that Defendant would use part of the monies paid to Zynga, or monies which it derived from advertising on its free games, under the implied contracts to fund adequate and reasonable data security practices.

142. Plaintiffs and class members would not have provided and entrusted their PII to Zynga or would have paid less for Zynga's services in the absence of the implied contract or implied terms between them and Zynga. The safeguarding of the PII of Plaintiffs and class members was critical to realize the intent of the parties.

143. Plaintiffs and class members fully performed their obligations under the implied contracts with Zynga.

144. Zynga breached its implied contracts with Plaintiffs and class members to protect their PII when it (1) failed to have security protocols and measures in place to protect that information; and (2) disclosed that information to unauthorized third parties.

145. As a direct and proximate result of these breaches of implied contract, Plaintiffs and class members sustained actual losses and damages as described in detail above, including but not limited to that they did not get the benefit of the bargain pursuant to which they provided their PII to Zynga

Count 8

CALIFORNIA UNFAIR COMPETITION LAW,

Cal. Bus. & Prof. Code §§ 17200, et seq.

Against Zynga on Behalf of Plaintiffs and the Nationwide Class

146. Plaintiffs repeat the allegations in paragraphs 1 – 78 in this Complaint, as if fully alleged herein.

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

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

149. Defendant's "unfair" acts and practices include:

a. Defendant failed to implement and maintain reasonable security measures to protect Plaintiffs' and the Nationwide Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Zynga Data Breach. Defendant failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security despite knowing the risk of cybersecurity incidents. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiffs and the Nationwide Class, whose PII has been compromised;

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

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

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

150. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Customer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, et seq., the FTC Act, 15 U.S.C. § 45, and California common law.

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

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and the Nationwide Class members' PII, which was a direct and proximate cause of the Zynga 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 Zynga Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the Nationwide Class members' PII, including duties imposed by the FTC Act, 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 Zynga Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and California Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the Nationwide Class members' PII, including duties imposed by the FTC Act and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and the Nationwide Class members' PII; and

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

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

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

154. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs' and the Nationwide Class members' rights. Defendant is of such a sophisticated and large nature that other data breaches and public information regarding security vulnerabilities put it on notice that its security and privacy protections were inadequate.

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

Count 9

MISSOURI MERCHANDISING PRACTICES ACT,

Mo. Rev. Stat. § 407.010, et seq.

Against Zynga on Behalf of Plaintiff Carol Johnson and the Missouri Subclass

156. Plaintiff Johnson repeats the allegations in paragraphs 1 – 78 in this Complaint, as if fully alleged herein.

157. Defendant violated Mo. Rev. Stat. § 407.010, et seq. ("MMPA") by engaging in unlawful, unfair, unconscionable and deceptive business acts and practices.

158. Defendant's unfair and unconscionable acts and practices include:

a. Defendant failed to implement and maintain reasonable security measures to protect Ms. Johnson's and the Missouri Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Zynga Data Breach. Defendant failed to identify foreseeable security risks, remediate identified

security risks, and adequately improve security despite knowing the risk of cybersecurity incidents. This conduct, with little if any utility, is unfair when weighed against the harm to Ms. Johnson and the Missouri Subclass, whose PII has been compromised;

b. Defendant's failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45 and Mo. Rev. Stat. § 407.1500.

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

d. Engaging in unlawful business practices by violating Mo. Rev. Stat. § 407.1500.

159. Defendant's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Ms. Johnson's and the Missouri Subclass members' PII, which was a direct and proximate cause of the Zynga 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 Zynga Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Ms. Johnson's and the Missouri Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Zynga Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Ms. Johnson's and Missouri Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Ms. Johnson's and the Missouri Subclass members' PII, including duties imposed by the FTC Act;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Ms. Johnson's and the Missouri Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Ms. Johnson's and the Missouri Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

161. As a direct and proximate result of Defendant's unfair, unconscionable, deceptive, and fraudulent acts and practices, Ms. Johnson and the Missouri Subclass members were injured and lost money or property: the money received by the Zynga for its services; the loss of the benefit of their bargain with and overcharges by Zynga as they would not have paid Zynga for services or would have paid less for such services but for the violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

162. Defendant acted intentionally, knowingly, and maliciously to violate Missouri's Merchandising Practices Act, and recklessly disregarded Ms. Johnson's and the Missouri Subclass members' rights. Defendant is of such a sophisticated and large nature that other data breaches and public information regarding security vulnerabilities put it on notice that its security and privacy protections were inadequate.

163. Ms. Johnson and the Missouri Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unconscionable, deceptive, and fraudulent business practices for use of their PII; declaratory relief; reasonable attorneys' fees and costs; injunctive relief; and other appropriate equitable relief.

Count 10

Wisconsin Deceptive Trade Practices Act,

Wisc. Stat. § 100.18, et seq.

Against Zynga on Behalf of Plaintiff Lisa Thomas and the Wisconsin Subclass

164. Plaintiff Thomas repeats the allegations in paragraphs 1 – 78 in this Complaint, as if fully alleged herein.

165. Zynga is a "person, firm, corporation or association," as defined by Wis. Stat. § 100.18(1).

166. Ms. Thomas and Wisconsin Subclass members are members of "the public," as defined by Wis. Stat. § 100.18(1).

167. With intent to sell, distribute, or increase consumption of merchandise, services, or anything else offered by Zynga to members of the public for sale, use, or distribution, Zynga made, published, circulated, placed before the public or caused (directly or indirectly) to be made, published, circulated, or placed before the public in Wisconsin advertisements, announcements, statements, and representations to the public which contained assertions, representations, or statements of fact which are untrue, deceptive, and/or misleading, in violation of Wis. Stat. § 100.18(1).

168. Zynga also engaged in the above-described conduct as part of a plan or scheme, the purpose or effect of which was to sell, purchase, or use merchandise or services not as advertised, in violation of Wis. Stat. § 100.18(9).

169. Zynga's Deceptive acts, practices, plans, and schemes include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Ms. Thomas' and Wisconsin Subclass members' PII, which was a direct and proximate cause of the Zynga Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Zynga Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Ms. Thomas' and Wisconsin Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Zynga Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Ms. Thomas' and Wisconsin Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Ms. Thomas' and Wisconsin Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Ms. Thomas' and Wisconsin Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Ms. Thomas' and Wisconsin Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

170. Zynga intended to mislead Ms. Thomas and Wisconsin Subclass members and induce them to rely on its misrepresentations and omissions.

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

172. Zynga had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extensivity of the PII in its possession. This duty arose because Ms. Thomas and the Wisconsin Subclass members reposed a trust and confidence in Zynga when they provided their Personal Information to Zynga in exchange for Zynga's services. In addition, such a duty is implied by

law due to the nature of the relationship between consumers—including Ms. Thomas and the Wisconsin Subclass—and Zynga, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Zynga. Zynga's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, while purposefully withholding material facts from Ms. Thomas and the Wisconsin Subclass that contradicted these representations.

173. Zynga's failure to disclose the above-described facts is the same as actively representing that those facts do not exist.

174. Zynga acted intentionally, knowingly, and maliciously to violate the Wisconsin Deceptive Trade Practices Act, and recklessly disregarded Ms. Thomas' and Wisconsin Subclass members' rights. Past data breaches of online businesses, including in the online gaming industry, put Zynga on notice that its security and privacy protections were inadequate.

175. As a direct and proximate result of Zynga's deceptive acts or practices, Ms. Thomas and Wisconsin Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including: the money received by the Zynga for its services; the loss of the benefit of their bargain with and overcharges by Zynga as they would not have paid Zynga for services or would have paid less for such services but for the violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

176. Zynga had an ongoing duty to all Zynga customers to refrain from deceptive acts, practices, plans, and schemes under Wis. Stat. § 100.18.

177. Ms. Thomas and Wisconsin Subclass members seek all monetary and non-monetary relief allowed by law, including damages, restitution, reasonable attorneys' fees, and costs under Wis. Stat. § 100.18(11)(b)(2), injunctive relief, and punitive damages.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendant as follows:

1) For an Order certifying the Nationwide Class and the Subclasses, as defined herein, and appointing Plaintiffs and Plaintiffs' counsel to represent the Classes as alleged herein;

2) For injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and class members, including but not limited to an order:

   a) Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

   b) Requiring Defendant to protect, including through adequate encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

   c) Requiring Defendant to delete, destroy, and purge the PII of Plaintiffs and class members unless Zynga can provide the Court a reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and the class members;

   d) Requiring Zynga to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and class members' PII;

   e) Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

   f) Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

   g) Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

   h) Requiring Defendant to conduct regular database scanning and security checks;

   i) Requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as

appropriate based upon employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiffs and class members;

j) Requiring Defendant to routinely and continually conduct internal training and education, at least annually, to inform security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

k) Requiring Defendant to implement, maintain, regularly review, and revise as necessary, a threat management program designed to appropriately monitor the Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

l) Requiring Defendant to meaningfully educate all class members about the threats they face as a result of the loss of their PII to third parties, as well as the steps affected individuals must take to protect themselves; and

m) Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers.

3) For an award of compensatory, consequential, and general damages, including nominal damages, as allowed by law in an amount to be determined;

4) For an award of statutory damages, trebeled, and punitive or exemplary damages, as allowed by law in an amount to be determined;

5) For an award of restitution or disgorgement, in an amount to be determined;

6) For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

7) For prejudgment interest on all amounts awarded; and

8) Such other and further relief as the Court may deem just and proper.

JURY DEMAND

Plaintiffs, on behalf of themselves and the Classes of all others similarly situated, hereby demand a trial by jury on all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

Dated: March 23, 2020

Respectfully submitted,

/s/ Hassan A. Zavareei

Hassan A. Zavareei (State Bar No. 181547)
Mark A. Clifford*
TYCKO & ZAVAREEI LLP
1828 L Street NW, Suite 1000
Washington, D.C. 20036
Telephone: (202) 973-0900
Facsimile: (202) 973-0950
Email: hzavareei@tzlegal.com
mclifford@tzlegal.com

Melissa S. Weiner*
Joseph C. Bourne (State Bar No. 308196)
PEARSON, SIMON & WARSHAW, LLP
800 LaSalle Avenue, Suite 2150
Minneapolis, Minnesota 55402
Telephone: (612) 389-0600
Facsimile: (612) 389-0610
Email: mweiner@pswlaw.com
jbourne@pswlaw.com

Jonathan M. Streisfeld*
Jeff Ostrow*
KOPELOWITZ OSTROW
FERGUSON WEISELBERG GILBERT
1 West Las Olas Blvd. Suite 500
Fort Lauderdale, FL 33301
Telephone: (954) 525-4100
Facsimile: (954) 525-4300
Email: streisfeld@kolawyers.com
ostrow@kolawyers.com

**pro hac vice* application forthcoming

Counsel for Plaintiffs and the Proposed Classes

CIVIL COVER SHEET

The JS-CAND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS
Carol Johnson and Lisa Thomas

(b) County of Residence of First Listed Plaintiff Greene County, MO
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Tycko & Zavareei LLP, 1828 L Street NW, Suite 1000, Washington, DC 20036 / (202) 973-0900

DEFENDANTS
Zynga, Inc.

County of Residence of First Listed Defendant San Francisco
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment Of Veteran's Benefits
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- ☐ 362 Personal Injury -Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury – Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities–Employment
- ☐ 446 Amer. w/Disabilities–Other
- ☐ 448 Education

PRISONER PETITIONS

HABEAS CORPUS
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

OTHER
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee–Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC § 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC § 158
- ☐ 423 Withdrawal 28 USC § 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent—Abbreviated New Drug Application
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS–Third Party 26 USC § 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC § 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced & Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation–Transfer ☐ 8 Multidistrict Litigation–Direct File

VI. CAUSE OF ACTION
Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)
Brief description of cause:
Claims for damages and injunctive relief arising from September 2019 data breach of Zynga, Inc.

VII. REQUESTED IN COMPLAINT:
✓ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, Fed. R. Civ. P.
DEMAND $ 5,000,000
CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S), IF ANY *(See instructions):*
JUDGE Hon. Laurel Beeler DOCKET NUMBER 3:20-cv-01539-LB

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)
(Place an "X" in One Box Only) ☒ **SAN FRANCISCO/OAKLAND** ☐ **SAN JOSE** ☐ **EUREKA-MCKINLEYVILLE**

DATE 03/23/2020 **SIGNATURE OF ATTORNEY OF RECORD** /s/ Hassan A. Zavareei

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

Authority For Civil Cover Sheet. The JS-CAND 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I. a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)."

II. Jurisdiction. The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.

(1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.

(2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

(3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.

(4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. Origin. Place an "X" in one of the six boxes.

(1) Original Proceedings. Cases originating in the United States district courts.

(2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.

(3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

(4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

(5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

(6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.

(8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket.

Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC § 553. Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Federal Rule of Civil Procedure 23.

Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.

Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

IX. Divisional Assignment. If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: "the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated."

Date and Attorney Signature. Date and sign the civil cover sheet.

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database