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

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

Attorneys for Plaintiff (Additional Counsel Listed on Signature Page)

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

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

Plaintiff,

v.

ZYNGA INC.,

Defendant.

Case No. 20-cv-5674

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Table of Contents

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

I. INTRODUCTION

1. Defendant Zynga Inc. ("Zynga") proclaims it is "a leading developer of the world's most popular social games that are played by millions of people around the world each day." Zynga promises that it has in place "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…."

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

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

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

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

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

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

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

II. PARTIES

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

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

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

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

III. JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 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 Zynga is a citizen of a state different from that of at least one Class member.

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

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

IV. INTRADISTRICT ASSIGNMENT

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

V. FACTS

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

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

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

---

[2] https://www.zynga.com/# (last visited 7/27/20).
[3] https://www.crunchbase.com/organization/zynga#section-overview (last visited 7/27/20).
[4] "Average monthly active users (MAU) of Zynga games from 4th quarter 2012 to 1st quarter 2020," found at https://www.statista.com/statistics/273569/monthly-active-users-of-zynga-games/ (last visited 7/27/20).
[5] "Words With Friends trumps Pokemon GO as most popular US mobile game in March 2017 with 13 million users" (5/4/17) found at https://www.pocketgamer.biz/news/65662/words-with-friends-13-million-users-march-2017/ (last visited 7/27/20).

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

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

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

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

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

B. Zynga collected PII from minors.

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

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

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

continues to be minors.

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

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

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

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

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

[8] Zynga Inc., Form 10-K, Fiscal Year Ended December 31, 2019, found at https://investor.zynga.com/static-files/d91122ee-c93f-468b-a48e-6d3b3c1441e3 (last visited 7/27/20).
[9] "Facebook knowingly duped game-playing kids and their parents out of money," (1/24/19), found at https://www.revealnews.org/article/facebook-knowingly-duped-game-playing-kids-and-their-parents-out-of-money/ (last visited 7/27/20).
[10] *Id.*
[11] "Documents Show Facebook Knowingly Took Money from Unwitting Children," (1/25/19), found at https://www.popularmechanics.com/technology/apps/a26041842/documents-show-facebook-knowingly-took-money-from-unwitting-children/ (last visited 7/27/20).
[12] "Identity Theft Poses Extra Troubles for Children," (4/17/15), found at https://www.nytimes.com/2015/04/18/your-money/a-childs-vulnerability-to-identity-theft.html?searchResultPosition=1 (last visited 7/27/20).

States."[13]

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

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

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

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

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

---

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

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

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

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

[17] "Password Breach of Game Developer Zynga Compromises 170 Million Accounts," *supra.*

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

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

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

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

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

---

[18] *Id.*

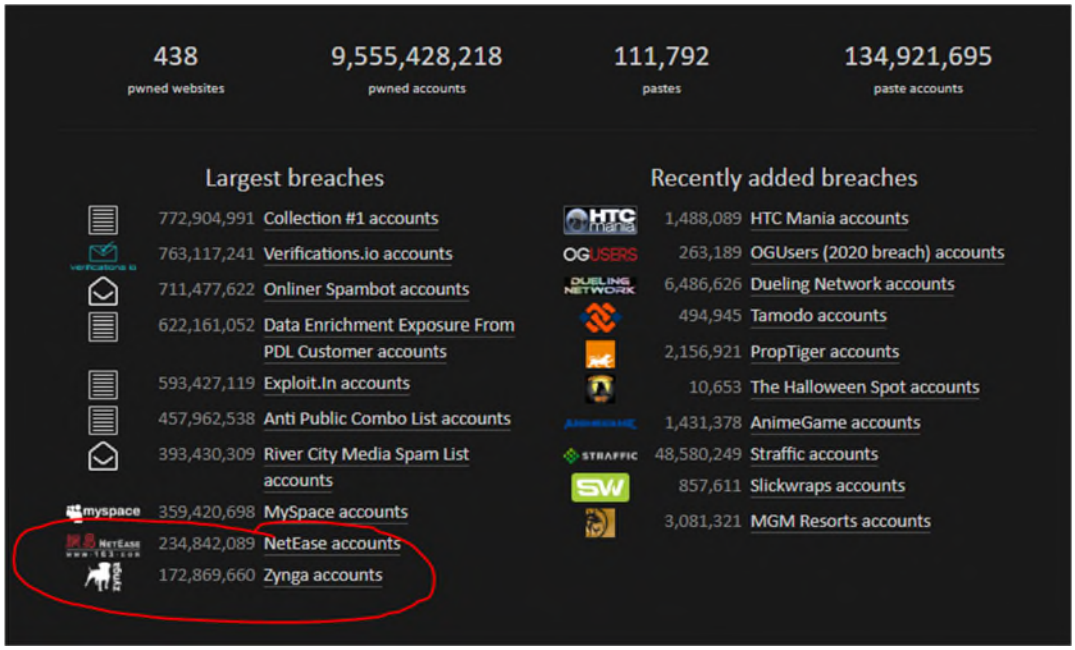
[19] Zynga Inc., Form 10-K, Fiscal Year Ended December 31, 2012, found at https://www.sec.gov/Archives/edgar/data/1439404/000119312513072858/d489727d10k.htm (last visited 7/27/20).

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

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

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

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



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

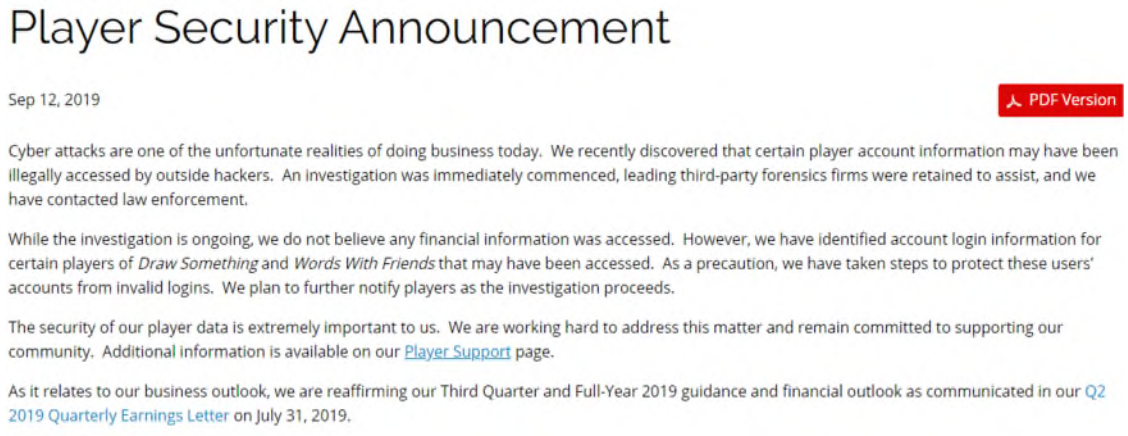
36. Zynga admitted that it had been breached in a September 12, 2019, statement posted on its website which it called a "Player Security Announcement." But Zynga did not accept responsibility for the attack and minimized its scope. Zynga suggested that hacking is unavoidable: "Cyber attacks are one of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

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

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

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

[25] *Id.*



Player Security Announcement

Sep 12, 2019

PDF Version

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

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

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

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

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

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

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

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

[26] *Id.*

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

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

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

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

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

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

---

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

[28] *Id*.

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

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

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

this breach) makes it impossible to determine if the actual account holder is the one logging in."[32]

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

48. Annual monetary losses for cybercrimes are estimated to range between $375 billion and $575 billion worldwide. In the United States in 2018, there were 3 million identity theft and fraud complaints filed with the Federal Trade Commission. Of those, 1.4 million were fraud related, and 25% of those reported that money was lost. The median amount consumer paid in those cases was $375.[33]

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

> In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[34]

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

[32] *Id.* (quoting Robert Prigge, President of Jumio, which provides biometric verification services).
[33] "Facts + Statistics: Identity theft and cybercrime," found at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited 7/27/20).
[34] "The President's Identity Theft Task Force, Combating Identity Theft, A Strategic Plan" (April 2007), p.11, found at https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf (last visited 7/27/20).

friends.[35]

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

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

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

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

> [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.[39]

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

---

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

[36] *Id*.

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

[38] "Identity Theft: The Aftermath 2017," *supra*, p.12.

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

mitigating the effects of the data breach.

VI. CLASS ACTION ALLEGATIONS

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

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

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

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

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

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

d. Whether Defendant failed to disclose the material facts that it did not have adequate security practices and systems to safeguard its customers' PII;

e. Whether Defendant failed to provide timely and adequate notice of the data breach;

f. Whether Defendant owed a duty to Plaintiff and Class members to protect their

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

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

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

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

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

k. Whether, as a result of Defendant's conduct, Plaintiff 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;

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

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

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

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

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

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

62. ***Superiority: Federal Rule of Civil Procedure 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 damages or other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford litigation, the court system could not. Individualized litigation creates a 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 single adjudication, economies of scale, and comprehensive supervision by a single court, especially where there are over 172 million Zynga users affected.

VII. CLAIMS

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

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

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

65. This duty included, among other things:

a. designing, maintaining, and testing its security systems to ensure that Plaintiff's and Class members' PII in its possession was adequately secured and protected;

b. implementing processes that would detect a breach of its security system in a timely manner;

c. timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks;

d. maintaining data security measures consistent with current technology and industry standards; and

e. timely notifying customers that their PII had been compromised, lost, stolen, accessed, or misused.

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

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

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

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

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

and thus was 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 Plaintiff and Class members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with current technology and industry standards; and (d) timely disclose that Plaintiff's and Class members' PII in Defendant's possession had been or was reasonably believed to have been, stolen or compromised.

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

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

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

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

a. theft of their PII;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

c. costs associated with purchasing credit monitoring and identity theft protection services;

d. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

89. Zynga breached its agreement with Plaintiff 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.

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

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

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

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

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

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

95. Plaintiff 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. Under the implied contracts, Plaintiff and Class members believed that Defendant would use part of the monies paid to Zynga or monies it derived from advertising to provide reasonable and adequate data security to protect Plaintiff's and Class members' PII.

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

97. Plaintiff and Class members fully performed their obligations under the implied contracts with Zynga.

98. Zynga breached its implied contracts with Plaintiff 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 implied agreement.

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

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

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

101. This claim is an alternative to Plaintiff's breach of contract and breach of implied contract claims.

102. Plaintiff and Class members have an equitable and legal interest in their PII that was conferred upon, collected by, and maintained by Defendant and that was ultimately stolen in the data breach.

103. Defendant benefited from the collection of Plaintiff and the Class' PII, and its ability to retain, use, and profit from that information. Defendant understood the benefit of collecting and possessing this information.

104. Defendant also understood that Plaintiff's and the Class' PII was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

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

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

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

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

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

110. As a result of Defendant's wrongful conduct including, among other conduct, its knowing failure to employ adequate data security measures, its continued maintenance and use Plaintiff's and Class members' PII 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, Plaintiff and Class members.

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

112. 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 Plaintiff 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.

113. 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.

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

115. Defendant is therefore liable to Plaintiff 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 Plaintiff 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 Plaintiff's and Class members' PII.

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

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

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

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

119. Plaintiff's and Class members provided their 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.

120. Plaintiff 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.

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

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

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

123. But for Defendant's disclosure of Plaintiff's 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 Plaintiff's and Class members' PII, as well as the resulting damages.

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

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

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

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

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

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

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

a. Failing to implement and maintain reasonable security measures to protect Plaintiff's and Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the data breach.

b. Failing to identify foreseeable security and privacy risks, remediate identified

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

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

d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45 and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., which was a direct and proximate cause of the data breach;

e. Failing to implement and maintain reasonable security measures, which led to substantial 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;

f. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82, by failing to disclose a data security breach and failing to notify or timely notify Plaintiff and Class members that their PII had been accessed and stolen;

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

h. Omitting, suppressing, and concealing the material fact that it did not reasonably

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

i. 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 Plaintiff's and Class members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45 and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.; and

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

130. Defendant has also 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 False Advertising Law, Cal. Bus. & Prof. Code §§ 17500, et seq., California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, et seq., the FTCA, 15 U.S.C. § 45, and California common law.

131. 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.

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

133. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff and Class members were injured and lost money or property: the money received by 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.

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

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

135. Plaintiff and 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; injunctive relief; and other appropriate equitable relief.

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

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

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

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

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

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

a. Failing to disclose that reasonable security measures to protect Plaintiff's and Class members' PII from unauthorized disclosure, release, data breaches, and theft, were in place, which was a direct and proximate cause of the data breach.

b. Failing to disclose foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the data breach. This conduct was unfair when weighed against the harm to Plaintiff and Class members, whose PII has been compromised;

c. Failing to disclose non-compliance with reasonable security measures, which was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTCA, 15 U.S.C. § 45, and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5;

d. Failing to disclose non-compliance with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45 and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., which was a direct and proximate cause of the data breach;

e. Failing to disclose non-compliance with reasonable security measures, which led to substantial 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;

f. Failing to disclose a data security breach in violation of Cal. Civ. Code §

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

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

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

i. 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 Plaintiff's and Class members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45 and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq..

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

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

142. 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.

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

144. As a direct and proximate result of Defendant's unlawful, untrue, misleading and deceptive advertising and practices, Plaintiff and Class members were injured and lost money or property: the money received by 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.

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

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

147. Plaintiff and 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;; injunctive relief; and other appropriate equitable relief.

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

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

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

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

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

a. Failing to disclose its failure to implement and maintain reasonable security measures to protect Plaintiff's and Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the data breach.

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the data breach. This conduct was unfair when weighed against the harm to Plaintiff and Class members, whose PII has been compromised;

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

d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45 and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., which was a direct and proximate cause of the data breach;

e. Failing to disclose its failure to implement and maintain reasonable security measures, which led to substantial 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;

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

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

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

i. 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 Plaintiff's and Class members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45 and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.; and

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

152. As a direct and proximate result of Defendant's unlawful acts and practices, Plaintiff and Class members were injured and lost money or property: the money received by 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.

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

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

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

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

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

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

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

a. the Alaska Unfair Trade Practices and Consumer Protection Act, Alaska Stat. § 45.50.471, et seq.;

b. the Arizona Consumer Fraud Act, Ariz. Rev. Stat. §§ 44-1521, et seq.;

c. the Arkansas Deceptive Trade Practices Act, Ark. Code § 4-88-101, et seq.;

d. the California Unfair Competition Law, Bus. & Prof. Code §§ 17200, et seq. and 17500, et seq.;

e. the California Consumers Legal Remedies Act, Cal. Civ. Code § 1750, et seq.;

f. the Colorado Consumer Protection Act, Colo. Rev. Stat. Ann. § 6-1-101, et seq.;

g. the Connecticut Unfair Trade Practices Act, Conn. Gen Stat. Ann. § 42- 110, et seq.;

h. the Delaware Consumer Fraud Act, 6 Del. Code § 2513, et seq.;

i. the D.C. Consumer Protection Procedures Act, D.C. Code § 28-3901, et seq.;

j. the Florida Deceptive And Unfair Trade Practices Act, Fla. Stat. Ann. § 501.201, et seq.;

k. the Georgia Fair Business Practices Act, Ga. Code Ann. § 10-1-390, et seq.;

l. the Hawaii Unfair Competition Law, Haw. Rev. Stat. § 480-2, et seq.;

m. the Idaho Consumer Protection Act, Idaho Code. Ann. § 48-601, et seq.;

n. the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 501/1, et seq.;

o. the Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5-2, et seq.;

p. the Iowa Consumer Fraud Act, Iowa Code § 714H, et seq.;

q. the Kansas Consumer Protection Act, Kan. Stat. Ann. § 50-623, et seq.;

r. the Kentucky Consumer Protection Act, Ky. Rev. Stat. Ann. § 367.110, et seq.;

s. the Louisiana Unfair Trade Practices And Consumer Protection Law, LSA-R.S. 51:1401, et seq.;

t. the Maine Unfair Trade Practices Act, Me. Rev. Stat. Ann. Tit. 5, § 207, et seq.;

u. the Maryland Consumer Protection Act, Md. Code Ann. Com. Law, § 13-301, et seq.;

v. the Massachusetts Regulation of Business Practices for Consumers Protection Act, Mass. Gen Laws Ann. Ch. 93A, et seq.;

w. the Michigan Consumer Protection Act, Mich. Comp. Laws Ann. § 445.901, et seq.;

x. the Minnesota Prevention of Consumer Fraud Act, Minn. Stat. § 325F, et seq.;

y. the Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407, et seq.;

z. the Nebraska Consumer Protection Act, Neb. Rev. St. §§ 59-1601, et seq.;

aa. the Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. § 41.600, et seq.

bb. the New Hampshire Regulation of Business Practices For Consumer Protection, N.H. Rev. Stat. § 358-A:1, et seq.;

cc. the New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8, et seq.;

dd. the New Mexico Unfair Practices Act, N.M. Stat. Ann. § 57-12-1, et seq.;

ee. the New York Consumer Protection from Deceptive Acts and Practices, N.Y. Gen. Bus. Law § 349, et seq.;

ff. the North Carolina Unfair And Deceptive Trade Practices Act, N.C. Gen Stat. § 75-1.1, et seq.;

gg. the North Dakota Consumer Fraud Act, N.D. Cent. Code § 51-15, et seq.;

hh. the Ohio Consumer Sales Practices Act, Ohio Rev. Code Ann. § 1345.01, et seq.;

ii. the Oklahoma Consumer Protection Act, Okla. Stat. tit. 15 § 751, et seq.;

jj. the Oregon Unlawful Trade Practices Act, Or. Rev. Stat. § 646.605, et seq.;

kk. the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. § 201-1, et seq.;

ll. the Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1-5.2(B), et seq.;

mm. the South Carolina Unfair Trade Practices Act, S.C. Code Ann. §§ 39-5- 10, et seq.;

nn. the South Dakota Deceptive Trade Practices and Consumer Protection, S.D. Codified Laws § 37-24-1, et seq.;

oo. the Tennessee Consumer Protection Act, Tenn. Code Ann. § 47-18-101, et seq.;

pp. the Texas Deceptive Trade Practices-Consumer Protection Act, Tex. Code Ann., Bus. & Con. § 17.41, et seq.;

qq. the Utah Consumer Sales Practices Act, Utah Code. Ann. § 13-11-175, et seq.;

rr. the Vermont Consumer Fraud Act, 9 V.S.A. § 2451, et seq.;

ss. the Virginia Consumer Protection Act of 1977, Va. Code Ann. § 59.1-199, et seq.;

tt. the Washington Consumer Protection Act, Wash. Rev. Code § 19.86.010, et seq.;

uu. the West Virginia Consumer Credit And Protection Act, W. Va. Code § 46A, et

seq.;

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

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

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

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

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

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

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

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

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

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

WHEREFORE, Plaintiff Christopher Rosiak respectfully requests that this Court:

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

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

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

d. Award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

e. Grant declaratory relief sought herein;

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

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

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

JURY DEMAND

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

Respectfully submitted,

DATED: August 13, 2020

By: */s/ Jennie Lee Anderson*

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

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

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

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

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

Attorneys for Plaintiff

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

Christopher Rosiak

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

JENNIE LEE ANDERSON
ANDRUS ANDERSON LLP
155 Montgomery Street, Suite 900, San Francisco, CA 94104
Telephone: (415) 986-1400

DEFENDANTS

Zynga Inc.

County of Residence of First Listed Defendant San Francisco County
(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:
Defendant did not take reasonable measures to prevent data breach of consumer identifying information.

VII. REQUESTED IN COMPLAINT:

✔ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, Fed. R. Civ. P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S), IF ANY *(See instructions):*

JUDGE Yvonne Gonzalez Rogers DOCKET NUMBER 20-cv-2612-YGR, 20-cv-1539- YGR, 20-cv-02024-YGR

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only) ☒ **SAN FRANCISCO/OAKLAND** ☐ **SAN JOSE** ☐ **EUREKA-MCKINLEYVILLE**

DATE 08/13/2020 **SIGNATURE OF ATTORNEY OF RECORD** /s/ Jennie Lee Anderson

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.

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

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

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

Plaintiff,

v.

ZYNGA INC.,

Defendant.

Case No. 20-cv-5674

DECLARATION OF JENNIE LEE ANDERSON PURSUANT TO CAL. CIVIL CODE § 1780(d)

I, Jennie Lee Anderson, declare as follow:

1. I am an attorney duly authorized to practice law in the State of California and this district. I represent the named plaintiff in this litigation.

2. I have personal knowledge of the matters set forth herein except as to those matters stated herein that are based upon information and belief. If called as a witness I could and would testify competently to these matters herein.

3. According to documents filed with the California Secretary of State, and on information and belief, Defendant Zynga Inc. resides and maintains its principal place of business in the City and County of San Francisco in the Northern District of California.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct and executed this 13th day of August 2020 in San Francisco, California.

/s/ Jennie Lee Anderson
Jennie Lee Anderson