Daniel L. Warshaw (CA Bar No. 185365)
PEARSON, SIMON & WARSHAW, LLP
15165 Ventura Boulevard, Suite 400
Sherman Oaks, CA 91403
Telephone: (818) 788-8300
Facsimile: (818) 788-8104
Email: dwarshaw@pswlaw.com

Attorneys for Plaintiff and the Proposed Class
(Additional Counsel on Signature Page)

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
WESTERN DIVISION

CONNOR BURNS,

individually and on behalf of all others similarly situated,

Plaintiff,

v.

MAMMOTH MEDIA, INC.,

Defendant.

Case No. 2:20-cv-4855

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Connor Burns ("Plaintiff" or "Connor"), individually and on behalf of all other persons similarly situated, and through his attorneys of record, alleges the following against Defendant Mammoth Media, Inc. ("Mammoth" or "Defendant") based upon personal knowledge with respect to himself, on information and belief derived from investigation of counsel, and review of public documents as to all other matters.

INTRODUCTION

1. Wishbone is a mobile application ("app") made by Defendant that is extremely popular among teens and young adults. In 2016, the website Mashable reported that Wishbone's user base is "roughly 80 percent 18 to 13 year olds and 20 percent 19 to 25 year olds."[1] Indeed, on the Wishbone website, Mammoth advertises the application as a way for "Brands" to "[p]romote[] your products to the cool kids."[2]

2. On January 25, 2016, when he was just 14 years old, Connor downloaded Wishbone. To use the application, Connor was required to create an account and provide personal information including, at a minimum, his email address, a username, and a password.

3. After using Wishbone for about three months, Connor deleted the app but did not delete this profile, meaning Defendant retained his personal information.

4. Approximately four years later, on May 23, 2020, Connor received an email from Defendant with the subject line: "Action Recommended on Wishbone: Security Incident Involving Your Personal Information." It informed him that "an unauthorized individual may have had access to Wishbone's database through stolen credentials," and "that some of the compromised data included usernames, emails,

[1] Saba Hamedy, *Teen social networking app Wishbone jumps into video*, Mashable (June 1, 2016), https://mashable.com/2016/06/01/wishbone-social-networking-app-for-teens-video/.

[2] *Wishbone – Compare Anything*, Mammoth Media, Inc., https://wishbone.io/ (last visited May 30, 2020).

phone numbers, timezone/region, full name, bio, gender, hashed passwords and profile pictures."[3] As set forth below, Defendant was not forthcoming as to the full scope of personal identifying information (herein, "PII") stolen in this "security incident" (herein, the "Data Breach").

5. Public reporting confirms that Connor was not the Data Breach's only victim. The "[p]ersonal data from some 40 million users" was stolen in the Data Breach.[4]

6. These 40 million users' PII, including Connor's, was initially posted for sale on the Dark Web. All 40 million users' PII was later leaked for free on the Dark Web by hacker(s) going by the name "ShinyHunters."[5]

7. As set forth below, Mammoth is responsible for allowing the Data Breach to occur because it failed to implement and maintain reasonable safeguards and failed to comply with industry-standard data security practices, contrary to the representations made in Mammoth's privacy statements.

8. During the duration of the Data Breach, Mammoth failed to detect the unauthorized third parties' access to its service, notice the massive amounts of data that were compromised, and failed to take any steps to investigate the red flags that should have warned Mammoth that its systems were not secure. As a result of Mammoth's failure to protect the PII it was entrusted with, Plaintiff and class members have been exposed to and/or are at a significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. Plaintiff and class members

---

[3] A copy of this May 23, 2020 email is attached as **Exhibit A**.

[4] Lee Mathews, *Hacker Swipes Data On 40 Million Users of Popular Wishbone App*, Forbes (May 22, 2020), https://www.forbes.com/sites/leemathews/2020/05/22/40-million-wishbone-accounts-hacked/#b8816ad385fe.

[5] Phil Muncaster, *Wishbone Breach: 40 Million Records Leaked on Dark Web*, infosecurity Group, https://www.infosecurity-magazine.com/news/wishbone-breach-40-million-records/ (last visited May 30, 2020).

have also lost the inherent value of their PII. This harm was compounded by Mammoth's failure to properly or timely notify its users of the Data Breach and its failure to disclose the extent of the PII compromised in the Data Breach.

PARTIES

9. Plaintiff Connor Burns is a nineteen-year-old citizen and resident of the State of Idaho, including at the time of the incidents described herein. Connor entrusted PII to Mammoth with the reasonable expectation and understanding that Mammoth would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized users, and would be timely notified of any data security incidents involving his PII should such occur.

10. Defendant Mammoth Media, Inc. is a California corporation with its principal place of business in Santa Monica, California. It makes a number of apps, including Wishbone. Mammoth describes Wishbone as "the social polling app where millions of teens create and vote in side-by-side poll cards on a daily basis – comparing anything from their favorite artists, TV shows, fashion & beauty trends, politics and more."[6]

JURISDICTION AND VENUE

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

12. This Court has personal jurisdiction over Mammoth because it is authorized to and regularly conducts business in California and is headquartered in Santa Monica, California.

[6] *Our Apps*, Mammoth Media, Inc., https://mammoth.la/apps (last visited May 30, 2020).

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.

FACTUAL ALLEGATIONS

Mammoth and Its Privacy and Data Security Representations

14. Mammoth markets itself as "The Social Entertainment Studio for Gen Z."[7] It "build[s], publish[es] and monetize[s] short-form entertainment through multiple apps and interactive formats."[8] Mammoth's apps are massively popular – as of 2019, Wishbone had 22 million monthly users.[9]

15. Mammoth collects significant amounts of PII from its millions of Wishbone users. Its Privacy Policy, last updated January 10, 2019, discloses that Mammoth collects the following PII from Wishbone Users: "name, email address, physical address, phone number, gender, date of birth or other information." Mammoth states that such information "is collected when you register with any of our Apps or Sites, make a purchase, order a subscription, create an account using login credentials from a third-party social networking service account (SNS Account), subscribe to updates, communicate with us or other users, or otherwise provide us with your contact information."[10] Mammoth also collects "location information," as well as "device identifier, advertising ID, user settings and the operating system of your device, as well as information about how you use our Services."[11]

16. Mammoth recognizes the risks posed by collecting such a vast treasure

---

[7] *Mammoth Media*, Mammoth Media, Inc., https://mammoth.la/ (last visited May 30, 2020).
[8] *Id.*
[9] Mike Jones, *How Mammoth Media Wrote the Playbook for GenZ's New Rules*, Science Inc. (March 9, 2019), https://www.science-inc.com/mammoth.html.
[10] *Privacy Policy*, Mammoth Media, Inc. (January 10, 2019), http://cdn.getwishboneapp.com/ui/wb_pp.pdf.
[11] *Id.*

trove of PII, stating at the top of its Privacy Policy that it "respects the sensitive nature of any personal information you provide to us."[12] Mammoth further represents that it "take[s] commercially reasonable steps to protect our customer's Personal Data against unauthorized disclosure or loss."[13]

Mammoth's Knowledge That It Was and Is a Target of Cyber Threats

17. Mammoth knew it was a prime target for hackers given the significant amount of sensitive PII collected from users of Wishbone and stored on its systems. Indeed, in 2017, Wishbone was the subject of a data breach in which "[a]n estimated 2.2 million email addresses and 287,000 cellphone numbers were stolen."[14] At the time, representatives of Mammoth[15] stated that "[m]aintaining the integrity of your personal information is extremely important to us. . . . [We] will continue to take appropriate action to prevent future similar incidents."[16]

18. Mammoth's knowledge is underscored by massive data breaches of other companies offering mobile applications or services popular with young users. For example, in December 2019, the mobile gaming company Zynga, Inc., maker of the popular apps such as Words With Friends and Draw Something announced a data

[12] *Id.*
[13] *Id.*
[14] Stefanie Fogel, *Popular teen social app Wishbone hacked*, endgadget (March 15, 2017), https://www.engadget.com/2017-03-15-wishbone-app-hacked.html.
[15] Wishbone was initially created under the auspices of the technology "incubator," Science Inc., which upon information and belief still retains an ownership interest in Mammoth although Mammoth now operates as an independent company. *See* Michael Jones, *Science Inc.-backed Mammoth Media Raises Series A From Greylock Partners*, Medium (Jan. 30, 2018), https://medium.com/@mjones/science-inc-backed-mammoth-media-raises-series-a-from-greylock-partners-4cf065f311ef.
[16] Stefanie Fogel, *Popular teen social app Wishbone hacked*, endgadget (March 15, 2017), https://www.engadget.com/2017-03-15-wishbone-app-hacked.html.

breach in which almost "173 million usernames and passwords were compromised."[17]

19. Yet another example is the August 2019 data breach of the StockX fashion and sneaker trading platform popular with teens, which exposed the personal data of over 6.8 million customers.[18] These are not isolated incidents; the number of data breaches is growing each year. According to a report by the Identity Theft Resource Center, "there were 1,473 data breaches [in 2019], a 17% increase over 2018's 1,257."[19]

20. Despite being a holder of PII for tens of millions of its users, most of whom are minors, Mammoth failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to their highly sensitive systems and databases. Mammoth had the resources to prevent a breach, but neglected to adequately invest in data security, despite its own history with data breaches and the growing number of well-publicized data breaches affecting mobile application developers.

21. Mammoth failed to undertake adequate analyses and testing of its own systems, training of its own personnel, and other data security measures to ensure that similar vulnerabilities were avoided or remedied and that Plaintiff's and class members' PII was protected.

The Data Breach

22. In January 2020, the first indications of the Data Breach arose when a

---

[17] Phil Muncaster, *Zynga Breach Hit 173 Million Accounts*, Infosecurity Magazine (Dec. 23, 2019), https://www.infosecurity-magazine.com/news/zynga-breach-hit-173-million/.

[18] Zack Whittaker, *StockX was hacked, exposing millions of customers' data*, TechCrunch (Aug. 3, 2019), https://techcrunch.com/2019/08/03/stockx-hacked-millions-records/

[19] Chris Morris, *Hackers had a banner year in 2019*, Fortune (Jan. 28, 2010), https://fortune.com/2020/01/28/2019-data-breach-increases-hackers/.

database of Wishbone users' PII was dumped on the dark web.[20] By March 2020, the database of approximately 40 million Wishbone users' PII was circulating for sale on the dark web.[21] In May 2020, the hacker(s) known as "Shiny Hunters" released the entire database for free.[22]

23. Plaintiff cannot say for certain when the Data Breach first occurred or when Mammoth became aware of the Data Breach – Mammoth still has not disclosed this information. Mammoth should have been aware no later than January 2020, when its users' PII first appeared on the dark web, and certainly no later than March 2020 when its users' PII was circulating widely for sale.

24. Yet, despite this knowledge, it was not until May 23, 2020 that Defendant sent an email to Wishbone users, including Connor, with the subject line: "Action Recommended on Wishbone: Security Incident Involving Your Personal Information." It informed users that "an unauthorized individual may have had access to Wishbone's database through stolen credentials," and "that some of the compromised data included usernames, emails, phone numbers, timezone/region, full name, bio, gender, hashed passwords and profile pictures."[23]

25. Mammoth's email was not forthcoming. Public reporting suggests that, in addition to the PII that was mentioned in Mammoth's May 23 email, "social media profiles" and "Facebook and Twitter access tokens" were stolen in the Data Breach.[24]

---

[20] Lawrence Abrams, *Hacker shares 40 million Wishbone user records for free*, BleepingComputer (May 21, 2020), https://www.bleepingcomputer.com/news/security/hacker-shares-40-million-wishbone-user-records-for-free/.

[21] *Id.*

[22] *Id.*

[23] A copy of this May 23, 2020 email is attached as **Exhibit A**.

[24] *Hackers post Sensitive Data of Wishbone Users on Darknet*, CISOMAG (May 22, 2020), https://www.cisomag.com/hackers-post-sensitive-data-of-wishbone-users-on-darknet/.

A review of a sample of the hacked Wishbone database identifies even more PII was stolen in the Data Breach: "uid, username, email, name, mobile_number, country_code, fbid, access_token, auth_token, ip, create_time, twitter_id, twitter_access_token, twitter_access_secret, gender, date_of_birth, password, image, follower_count, device_token, android_device_token, is_admin, timezone, displaying_post_date, is_device_active, shared_for_date, show_second_session_date, apple_idfa, google_advertiser_id, stickers_left, deleted_at, [and] updated_at."[25]

26. Reporting also uncovered that the "hashed passwords" stolen in the Data Breach and referenced in Mammoth's May 23, 2020, email were in fact hashed with the MD5 algorithm. "MD5 was declared 'cryptographically broken' by experts" back in 2010. "A moderately-complex password hashed with MD5 could be cracked in 30 minutes or less."[26]

27. The inadequacy of Mammoth's MD5 encryption was explained by Trevor Morgan, Product Manager with data security company comforte AG:

> If data tokenization had been applied to the personal information of the 40 million registered Wishbone users, then they may have avoided a serious scandal which saw valuable information such as email addresses, phone numbers and usernames breached. Tokenizing this data would have rendered that sensitive information meaningless to a hacker or bad actor and therefore worthless to any potential buyers. Unfortunately, in this case the stolen passwords were in MD5 format, a weak form of password hashing which can be decoded by malicious actors and therefore monetized through sale on hacking forums. Encrypted or tokenized data, however, could not be listed for sale on the dark web because it becomes undecipherable without the necessary key, therefore

[25] Lawrence Abrams, *supra* note 21.
[26] Lee Matthews, *supra* note 4.

> reducing the likelihood of data exposure during a breach, and maintaining the security of valuable personal information.[27]

28. Mr. Morgan's observations were echoed by Mark Bower, Senior Vice President of comforte AG:

> It looks like security and privacy have been an afterthought, not a matter of culture and software development process. If the passwords are hashed with MD5, then the users affected should be immediately making sure their ID's and passwords aren't used elsewhere with the same password. MD5 is a goner as far as security is concerned but used by mistaken developers unfamiliar with its security risks, or using older code libraries using MD5. Hashed MD5 passwords aren't difficult to brute force. The bigger issue here is the personal data though – so now attackers have a bunch more data for social engineering. Really though, given the scale, why wasn't the data tokenized to de-identify it? 40 million is a lot, but it's really not hard even at high volume to snap tokenization into an existing data capture process. There's no need to have PII sitting around in server or cloud databases – and most analytics and operations can run on de-identified data which would avoid this massive breach from having any meaningful impact.[28]

29. Mammoth has been silent since its May 23, 2020 email and has not offered victims of the Data Breach any type of identity or fraud monitoring or identity theft protection services. Notably, other companies have provided identity-theft protection services to victims of similar breaches.

---

[27] Security Experts, *Expert Insight on Wishbone App Data Breach Affects 40m Users*, isBuzznews (May 22, 2020), https://www.informationsecuritybuzz.com/expert-comments/experts-insight-on-wishbone-app-data-breach-affects-40m-users/.

[28] *Id.*

30. Mammoth's delayed and inadequate response to the Data Breach has caused harm and confusion among victims of the Data Breach, causing class members to spend time, and continuing to spend a significant amount of time into the future, taking measures to identify the scope of their exposure and protect themselves from identity theft, fraud, and other identity-related crimes.

31. Mammoth is responsible for allowing the Data Breach to occur because it failed to implement and maintain any reasonable safeguards and failed to comply with industry-standard data security practices, contrary to the representations made in Mammoth's privacy statements.

32. During the duration of the Data Breach, Mammoth failed to detect the unauthorized third parties' access to its systems and databases, notice the massive amounts of data that were compromised, and failed to take any steps to investigate the red flags that should have warned Mammoth that its systems were not secure. As a result of Mammoth's failure to protect the sensitive PII it was entrusted with, Plaintiff and class members are at a significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. Plaintiff and class members have also lost the inherent value of their PII.

33. Plaintiff and class members provided their PII to Mammoth with the expectation and understanding that Mammoth would adequately protect and store their data. If Plaintiff and class members had known that Mammoth's data security was insufficient to protect their PII, they would not have entrusted their PII to Mammoth, created a Wishbone user account, downloaded Wishbone, and would not have been willing to pay for, or pay as much for any in-app purchases.

Mammoth Failed to Comply with Regulatory Guidance and Meet Consumers' Expectations

34. Federal agencies have issued recommendations and guidelines to temper data breaches and the resulting harm to individuals and financial institutions. For

example, the FTC has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[29]

35. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[30] Among other things, the guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[31]

36. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[32]

37. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to

---

[29] Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited May 26, 2020).

[30] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[31] *Id.*

[32] FTC, *Start With Security*, *supra* note 27.

confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[33]

38. In this case, Mammoth was fully aware of its obligation to use reasonable measures to protect the PII of its users, acknowledging as much in its own Privacy Policy. Mammoth also knew it was a target for hackers. But despite understanding the consequences of inadequate data security, Mammoth failed to comply with industry-standard data security requirements.

39. Mammoth's failure to employ reasonable and appropriate measures to protect against unauthorized access to its users' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45 and various state consumer protection and data breach statutes.

Effect of the Data Breach

40. Mammoth's failure to keep Plaintiff's and class members' PII secure has severe ramifications. Given the sensitive nature of the PII stolen in the Data Breach, cyber criminals have the ability to commit identity theft and other identity-related fraud against Plaintiff and class members now and into the indefinite future.

41. The information stolen from Mammoth included usernames and passwords—PII that is highly valued among cyber thieves and criminals on the Dark Web. For example, Apple ID usernames and passwords were sold on average for $15.39 each on the Dark Web, making them the most valuable non-financial credentials for sale on that marketplace. Usernames and passwords for eBay ($12),

[33] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited May 26, 2020).

Amazon (≤$10), and Walmart (≤$10) fetch similar amounts.[34] Consumers often reuse passwords. By unlawfully obtaining this information, cyber criminals can use these credentials to access other services beyond that which was hacked.

42. PII also has significant monetary value in part because criminals continue their efforts to obtain this data.[35] In other words, if any additional breach of sensitive data did not have incremental value to criminals, one would expect to see a reduction in criminal efforts to obtain such additional data over time. Instead, just the opposite has occurred. For example, the Identity Theft Resource Center reported 1,473 data breaches in 2019, which represents a 17 percent increase from the total number of breaches reported in 2018.[36]

43. The harm caused by the accumulation of data from prior data breaches has been articulated by numerous cyber and data security experts following the Data Breach. For example, Jake More, Cybersecurity Specialist with the internet security company ESET explained:

> Even hashed passwords can be cracked. If a criminal hacker succeeds in accessing a hashed password database, it can be placed in a table of passwords that have been already hashed. Therefore, if that password has been used before and hashed, it can essentially be reverse engineered to match a previous hash value. When you add connecting email addresses

---

[34] Don Reisinger, *Here's How Much Your Stolen Apple ID Login Costs on the Dark Web*, Fortune (March 7, 2018), https://fortune.com/2018/03/07/apple-id-dark-web-cost/. *See also* https://www.npr.org/2018/02/22/588069886/take-a-peek-inside-the-market-for-stolen-usernames-and-passwords (last visited May 26, 2020).

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

[36] *2019 End-of-Year Data Breach Report* (2019), Identity Theft Resource Center, *available at* https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf.

> to those now cracked passwords, attackers are then able to attempt to access other online services such as bank accounts, email address and others if those accounts reuse the same password.[37]

44. Javvad Malik with the cybersecurity company KnowBe4 further illustrates the problem, noting that once "attackers get hold of emails addresses and passwords, they can use those to try attacking other websites that the user is registered to with password stuffing. Or they can go directly after the user with phishing attacks."[38]

45. Moreover, the value of PII is key to unlocking many parts of the financial sector for consumers. Whether someone can obtain a mortgage, credit card, business loan, tax return, or even apply for a job depends on the integrity of their PII. Similarly, the businesses that request (or require) consumers to share their PII as part of a commercial transaction do so with the expectation that its integrity has not been compromised.

46. Annual monetary losses for victims of identity theft are in the billions of dollars. In 2017, fraudsters stole $16.8 billion from consumers in the United States, which includes $5.1 billion stolen through bank account take-overs.[39]

47. The annual cost of identity theft is even higher. McAfee and the Center for Strategic and International Studies estimates that the likely annual cost to the global economy from cybercrime is $445 billion a year.[40]

48. The foregoing problems are compounded where, as with the majority of

---

[37] Security Experts, *supra* note 28.
[38] *Id.*
[39] Javelin, *2018 Identity fraud: Fraud Enters A New Era of Complexity*, available at https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity (last visited May 26, 2020).
[40] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited May 26, 2020).

Wishbone's users, the victims of the Data Breach are minors.

49. Over 1 million minor children were victims of fraud or identity theft in 2017, and two/thirds of those victims were under the age of seven.[41]

50. Data thieves are also more likely to target minors' PII and to use that PII once it is stolen. In 2017, "[a]mong notified breach victims . . . 39 percent of minors became victims of fraud, versus 19 percent of adults."[42]

51. Criminals make use of minors' PII to open accounts or new lines of credit that may not be noticed by the minor; and to create "synthetic identities" using a combination of real and fictitious information which again, the minor may not realize was stolen.[43] Because minors do not regularly monitor their bank accounts (if they have them) or their credit reports, data thieves are more likely to make unrestricted use of this information for longer periods of time than they would for adult victims.[44]

52. Minors also generally are less likely to receive notice from the company responsible for the data breach or to even realize that a thief has made fraudulent use of their information in other ways – such as creating a new identity for the purposes of accessing government benefits, healthcare, or employment.[45] Minors often "won't find out that their identity has been stolen until they apply for their first credit card or college loan."[46]

---

[41] Kelli B. Grant, *Identity Theft isn't just an adult problem. Kids are victims, too*, CNBC (April 24, 2018), https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html.

[42] *Id.*

[43] *Id.*

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

[45] *Id.*

[46] Larry Magid, *Teens Vulnerable to Identity Theft, Financial Crimes, and Impersonation*, Forbes (Nov. 7, 2013),

53. Children are also particularly susceptible to physical harm in the event of a data breach. Data thieves can use their PII "to link a child to his or her parents and pinpoint the child's physical address."[47] This risk is particularly disturbing in light of the PII stolen in the Data Breach, which included location and social media profile information.

54. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, in addition to the irreparable damage that may result from the theft of PII, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[48]

55. Even before the occurrence of identity theft, victims may spend valuable time and suffer from the emotional toll of a data breach. Indeed, Connor has already begun to experience negative consequences as a result of the Data Breach. On May 22, 2020 (the day before Mammoth sent its inadequate and delayed notification of the Data Breach to Wishbone users), Connor received emails from the popular music service Spotify indicating that an unauthorized third party had accessed his account and changed his Spotify password. The compromise of his Spotify account was particularly disturbing to Connor as it could reveal not only his personal music listening history, but also other PII stored in his Spotify account which has now been exposed

---

https://www.forbes.com/sites/larrymagid/2013/11/07/teens-concerned-about-identity-theft/#6ab243211c49.

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

[48] U.S. Department of Justice, *Victims of Identity Theft, 2014* (Revised November 13, 2017), available at http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited May 26, 2020).

yet again to unauthorized third parties. Connor was forced to reset his Spotify login information, and he also spent time changing his passwords for his online accounts with Apple, Google, Amazon, and his financial institution. Connor also called Equifax, Experian, and TransUnion to place fraud alerts on his accounts. Moreover, since receiving notice of the Data Breach, Connor has spent time reviewing transactions on his bank account to ensure none were fraudulent. To date, Connor has spent about three hours of his time addressing the consequences of the Data Breach. He is concerned other accounts or aspects of his identity may be at risk, and will continue spending time to address the fallout from the Data Breach.

56. The impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans or mortgages.[49] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

57. It is no wonder, then, that identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey[50] evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear related to personal financial safety;
- 37% reported fearing for the financial safety of family members;

[49] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, available at https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited May 26, 2020).

[50] *Id.*

- 24% reported fear for their physical safety;
- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft; and
- 7% reported feeling suicidal.

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

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate / lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[51]

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[52]

---

[51] *Id.*

[52] U.S. Government Accountability Office, *Report to Congressional Requesters* (June 2007), http://www.gao.gov/new.items/d07737.pdf.

60. The risk of identity theft is particularly acute where detailed personal information is stolen, such as the PII that was compromised in the Data Breach.

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

a. identity theft and fraud resulting from theft of their PII;

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

c. losing the inherent value of their PII;

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

e. unauthorized access to and misuse of their online accounts;

f. 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;

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

h. costs associated with time spent and the loss of productivity or enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, addressing other varied instances of identity theft – such as credit cards, bank accounts, loans, government benefits, and other services procured using the stolen PII, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, updating login

information for online accounts sharing the same login credentials as were compromised in the Data Breach, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach;

i. the continued imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being in the possession of one or more unauthorized third parties; and

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

62. Additionally, Plaintiff and class members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[53]

63. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, companies like Mammoth would have no reason to tout their data security efforts to their actual and potential customers.

64. Had the victims of the Data Breach including Connor known the truth about Mammoth's data security practices—that Mammoth would not adequately

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

protect and store their PII—they would not have entrusted their PII to Mammoth, created a Wishbone user account, downloaded Wishbone, and would not have been willing to pay for, or pay as much for any in-app purchases.

65. Plaintiff and class members are at an imminent risk of fraud, criminal misuse of their PII, and identity theft for years to come as result of the Data Breach and Mammoth's deceptive and unconscionable conduct.

CLASS ACTION ALLEGATIONS

66. Pursuant to Federal Rule of Civil Procedure 23(b)(1), (b)(2) and (b)(3), Plaintiff seeks certification of the following Nationwide Class:

67. **Nationwide Class:** All individuals in the United States whose PII was compromised in the Data Breach.

68. The Nationwide Class (also referred to as the "Class") asserts claims against Mammoth for negligence (Count 1), negligence *per se* (Count 2), declaratory judgment (Count 3), breach of confidence (Count 4), intrusion upon seclusion (Count 5), violation of California's Unfair Competition Law (Count 6), and violations of state data breach statutes (Count 7).

69. Excluded from the Class are Mammoth, any entity in which Mammoth has a controlling interest, and Mammoth's officers, directors, legal representatives, investors, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officer presiding over this matter, members of their immediate family, members of their judicial staff, and any judge sitting in the presiding court system who may hear an appeal of any judgment entered.

70. **Risk of Inconsistent or Varying Adjudications. Fed. R. Civ. P. 23(b)(1).** As the proposed class members include millions of individuals, there is significant risk of inconsistent or varying adjudications with respect to individual class members that would establish incompatible standards of conduct for Mammoth. For example, injunctive relief may be entered in multiple cases, but the ordered relief may

vary, causing Mammoth to have to choose between differing means of upgrading its data security practices and choosing the court order with which it will comply. Class action status is also warranted because prosecution of separate actions by the members of the Class would create a risk of adjudications with respect to individual members of the Class that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

71. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of class members is unknown to Plaintiff at this time, approximately 40 million Wishbone users' PII was compromised in the Data Breach, suggesting the Class will number in the tens of millions.

72. **Commonality and Predominance. Fed. R. Civ. P. 23(a)(2) and (b)(3).** This action involves common questions of law and fact that predominate over any questions affecting individual class members. The common questions include, but are not limited to:

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

b. Whether Mammoth omitted or misrepresented material facts regarding the security of its computer and data storage systems and their inability to protect vast amounts of sensitive data, including Plaintiff's and class members' PII;

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

d. Whether Mammoth failed to take available steps to prevent and stop the Data Breach from happening;

e. Whether Mammoth failed to disclose the material facts that it did not

have adequate computer systems and security practices to safeguard PII;

f. Whether Mammoth owed duties to Plaintiff and class members to protect their PII;

g. Whether Mammoth owed a duty to provide timely and accurate notice of the Data Breach to Plaintiff and class members;

h. Whether Mammoth breached its duties to protect the PII of Plaintiff and class members by failing to provide adequate data security;

i. Whether Mammoth breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and class members;

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

k. Whether Mammoth was negligent, reckless, or intentionally indifferent in its representations to Plaintiff and class members concerning its security protocols;

l. Whether Mammoth's conduct and practices described herein amount to acts of intrusion upon seclusion;

m. Whether Mammoth was negligent in establishing, implementing, and following security protocols;

n. Whether Plaintiff's and class members' PII was compromised and exposed as a result of the Data Breach and the extent of that compromise and exposure;

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

p. Whether Mammoth's conduct amounted to violations of consumer protection and data breach statutes;

q. Whether, as a result of Mammoth'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;

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

s. Whether Plaintiff and class members are entitled to compensatory damages and statutory damages; and

t. Whether the Plaintiff and class members are entitled to punitive damages.

73. **Typicality. Fed. R. Civ. P. 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.

74. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Class. Plaintiff is a member of the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation and consumer protection claims. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the interests of the Class.

75. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs and class members may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the class members are relatively small compared to the burden and expense required to individually litigate their claims against Mammoth, and thus, individual litigation to redress Mammoth's wrongful conduct would be impracticable. Individual litigation by each class member would also strain the court system. Moreover, individual litigation creates the potential for inconsistent

or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

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

CAUSES OF ACTION

Count 1

NEGLIGENCE

Against Mammoth on Behalf of Plaintiff and the Nationwide Class

77. Plaintiff repeats the allegations in paragraphs 1 – 76 in this Complaint, as if fully alleged herein.

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

security systems and data storage architecture in a timely manner; (c) timely acting on all warnings and alerts, including public information, regarding Mammoth's security vulnerabilities and potential compromise of the PII of Plaintiff and class members; (d) maintaining data security measures consistent with industry standards and applicable state and federal law; and (e) timely and adequately informing Plaintiff and class members if and when a data breach occurred notwithstanding undertaking (a) through (d) above.

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

80. Mammoth had a duty to monitor, supervise, control, or otherwise provide oversight to safeguard the PII that was collected, stored, and processed by Mammoth's computer systems.

81. Mammoth's duties to use reasonable security measures also arose as a result of the special relationship that existed between Mammoth, on the one hand, and Plaintiff and class members, on the other hand. The special relationship arose because Plaintiff and class members entrusted Mammoth with their PII when creating and using Wishbone accounts. Mammoth alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

82. Mammoth's duties to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as

interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII. Various FTC publications and data security breach orders further form the basis of Mammoth's duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

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

84. Mammoth knew or should have known that a breach of its systems and data storage architecture would inflict millions of dollars of damages upon Plaintiff and the Class, and Mammoth was therefore charged with a duty to adequately protect this critically sensitive information.

85. Mammoth breached the duties it owed to Plaintiff and class members described above, and thus was negligent. Mammoth 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; and (c) maintain security systems consistent with industry standards.

86. Mammoth also failed to exercise reasonable care when it failed to timely notify Plaintiff and class members of the Data Breach and when it falsely conveyed information regarding the scope of the Data Breach in its May 23, 2020 email to Wishbone users.

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

88. As a direct and proximate result of Mammoth's negligence, Plaintiff and class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting

in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Mammoth, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

Count 2

NEGLIGENCE *PER SE*

Against Mammoth on Behalf of Plaintiff and the Nationwide Class

89. Plaintiff repeats the allegations in paragraphs 1 – 76 in this Complaint, as if fully alleged herein.

90. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Mammoth of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Mammoth's duty.

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

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

93. Plaintiff and class members are consumers within the class of persons

Section 5 of the FTC Act (and similar state statutes) were intended to protect.

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

95. As a direct and proximate result of Mammoth's negligence, Plaintiff and class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Mammoth, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

Count 3

DECLARATORY JUDGMENT

Against Mammoth on Behalf of Plaintiff and the Nationwide Class

96. Plaintiff repeats the allegations in paragraphs 1 – 76 in this Complaint, as if fully alleged herein.

97. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, the Court is authorized to enter a judgment declaring the rights and legal relations of the parties

and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

98. An actual controversy has arisen in the wake of the Data Breach regarding Mammoth's present and prospective common law and other duties to reasonably safeguard its users' PII, and whether Mammoth is currently maintaining data security measures adequate to protect Plaintiff and class members from further data breaches that compromise their PII. Plaintiff and class members remain at imminent risk that further compromises of their PII will occur in the future. This is true even if they are not actively using Mammoth's products or services.

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

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

b. Mammoth continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiff's and class members' PII.

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

101. If an injunction is not issued, Plaintiff and class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of Mammoth. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiff and class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

102. The hardship to Plaintiff and class members if an injunction does not

issue exceeds the hardship to Mammoth if an injunction is issued. Among other things, if another data breach occurs at Mammoth, Plaintiff and class members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Mammoth of complying with an injunction by employing reasonable data security measures is relatively minimal, and Mammoth has a pre-existing legal obligation to employ such measures.

103. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Mammoth, thus eliminating additional injuries that would result to Plaintiff, class members, and the tens of millions Wishbone users whose PII would be further compromised.

Count 4

BREACH OF CONFIDENCE

Against Mammoth on Behalf of Plaintiff and the Nationwide Class

104. Plaintiff repeats the allegations in paragraphs 1 – 76 in this Complaint, as if fully alleged herein.

105. At all times during Plaintiff's and class members' interactions with Mammoth, Mammoth was fully aware of the confidential and sensitive nature of Plaintiff's and class members' PII.

106. As alleged herein and above, Mammoth's relationship with Plaintiff and class members was governed by expectations 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.

107. Plaintiff and class members provided their respective PII to Mammoth with the explicit and implicit understandings that Mammoth would protect and not permit their PII to be disseminated to the public or any unauthorized parties.

108. Plaintiff and class members also provided their respective PII to

Mammoth with the explicit and implicit understandings that Mammoth would take precautions to protect the PII from unauthorized disclosure, such as following basic principles of encryption and information security practices.

109. Mammoth 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.

110. Due to Mammoth's failure to prevent, detect, and avoid the Data Breach from occurring by following best information security practices to secure Plaintiff's and class members' PII, Plaintiff's and class members' PII was disclosed and misappropriated to the public and unauthorized third parties beyond Plaintiff's and class members' confidence, and without their express permission.

111. But for Mammoth'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/or used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiff's and class members' PII, as well as the resulting damages.

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

113. As a direct and proximate result of Mammoth's breach of confidence, Plaintiff and class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and

other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Mammoth, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

Count 5

INTRUSION UPON SECLUSION

Against Mammoth on Behalf of Plaintiff and the Nationwide Class

114. Plaintiff repeats the allegations in paragraphs 1 – 76 in this Complaint, as if fully alleged herein.

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

116. Plaintiff and class members had a reasonable expectation of privacy in the PII that Mammoth mishandled.

117. By failing to keep Plaintiff's and class members' private information safe, and by misusing and/or disclosing said private information to unauthorized parties for unauthorized use, Mammoth invaded Plaintiff's and class members' privacy by:

a. Intruding into Plaintiff's and class members' private affairs in a manner that would be highly offensive to a reasonable person; and

b. Publicizing private facts about Plaintiff and class members, which is highly offensive to a reasonable person.

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

119. Mammoth invaded Plaintiff's and class members' right to privacy and intruded into Plaintiff's and class members' private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

120. As a proximate result of such misuse and disclosures, Plaintiff's and class members' reasonable expectation of privacy in their private information was unduly frustrated and thwarted. Mammoth's conduct amounted to a serious invasion of Plaintiff's and class members' protected privacy interests.

121. In failing to protect Plaintiff's private information, and in misusing and/or disclosing their private information, Mammoth has acted with malice and oppression and in conscious disregard of Plaintiff's and class members' rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing its own economic, corporate, and legal interests above the privacy interests of its tens of millions of users. Plaintiff and class members, therefore, seek an award of damages, including punitive damages, on behalf of Plaintiff and the Class.

Count 6

CALIFORNIA'S UNFAIR COMPETITION LAW

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

Against Mammoth on Behalf of Plaintiff and the Nationwide Class

122. Plaintiff repeats the allegations in paragraphs 1 – 76 in this Complaint, as

if fully alleged herein.

123. Mammoth is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

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

125. Mammoth's unfair acts and practices include:

a. Mammoth failed 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. Mammoth failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents in the education sector. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and class members whose PII has been compromised.

b. Mammoth's failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 *et seq.*, and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq.

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

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

126. Mammoth has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100, *et seq.*, and California common law.

127. Mammoth's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and class members' PII, 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 following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. 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 FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*, and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100, *et seq.*, which was a direct and proximate cause of the Data Breach;

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

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and class

members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45; California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*; and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 *et seq.*

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

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45; California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*; and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 *et seq.*

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

129. Mammoth intended to mislead Plaintiff and class members and induce them to rely on its misrepresentations and omissions.

130. Had Mammoth disclosed to Plaintiff and class members that its data systems were not secure and, thus, vulnerable to attack, Mammoth would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Mammoth received, maintained, and compiled Plaintiff's and class members' PII as part of the services and goods Mammoth provided and for which its users paid (either through in-app purchases or through the inherent value of their PII) without advising Plaintiff and class members that Mammoth's data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and class members' PII. Accordingly, Plaintiff and class members acted reasonably in relying on Mammoth's misrepresentations and omissions, the truth of which they could not have discovered.

131. Mammoth acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and class members' rights. A past breach of Mammoth's Wishbone application, as well as numerous breaches targeting apps and websites popular with teens, put Mammoth on notice that its security and privacy protections were inadequate.

132. As a direct and proximate result of Mammoth's unfair, unlawful, and fraudulent acts and practices, Plaintiff and class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages as described herein and as will be proved at trial.

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

Count 7

VIOLATION OF STATE DATA BREACH STATUTES

Against Mammoth on Behalf of Plaintiff and the Nationwide Class

134. Plaintiff repeats the allegations in paragraphs 1 – 76 in this Complaint, as if fully alleged herein.

135. Mammoth is a business that owns, maintains, and licenses PII, and computerized data including PII, about Plaintiff and class members.

136. Mammoth is in possession of PII belonging to Plaintiff and class members and is responsible for reasonably safeguarding that PII consistent with the requirements of the applicable laws pertaining thereto.

137. Mammoth knowingly and/or reasonably believing that Plaintiff's and class members' PII was acquired by unauthorized persons during the Data Breach, failed to provide reasonable and timely notice of the Data Breach to Plaintiff and class

members as required by the following data breach statutes.

138. Mammoth's failure to provide timely and accurate notice of the Data Breach violated the following state data breach statutes:

a. Alaska Stat. Ann. § 45.48.010(a), *et seq.*;

b. Ark. Code Ann. § 4-110-105(a), *et seq.*;

c. Cal. Civ. Code § 1798.83(a), *et seq.*;

d. Colo. Rev. Stat. Ann § 6-1-716(2), *et seq.*;

e. Conn. Gen. Stat. Ann. § 36a-701b(b), *et seq.*;

f. Del. Code Ann. Tit. 6 § 12B-102(a), *et seq.*;

g. D.C. Code § 28-3852(a), *et seq.*;

h. Fla. Stat. Ann. § 501.171(4), *et seq.*;

i. Ga. Code Ann. § 10-1-912(a), *et seq.*;

j. Haw. Rev. Stat. § 487N-2(a), *et seq.*;

k. Idaho Code Ann. § 28-51-105(1), *et seq.*;

l. Ill. Comp. Stat. Ann. 530/10(a), *et seq.*;

m. Iowa Code Ann. § 715C.2(1), *et seq.*;

n. Kan. Stat. Ann. § 50-7a02(a), *et seq.*;

o. Ky. Rev. Stat. Ann. § 365.732(2), *et seq.*;

p. La. Rev. Stat. Ann. § 51:3074(A), *et seq.*;

q. Md. Code Ann., Commercial Law § 14-3504(b), *et seq.*;

r. Mass. Gen. Laws Ann. Ch. 93H § 3(a), *et seq.*;

s. Mich. Comp. Laws Ann. § 445.72(1), *et seq.*;

t. Minn. Stat. Ann. § 325E.61(1)(a), *et seq.*;

u. Mont. Code Ann. § 30-14-1704(1), *et seq.*;

v. Neb. Rev. Stat. Ann. § 87-803(1), *et seq.*;

w. Nev. Rev. Stat. Ann. § 603A.220(1), *et seq.*;

x. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), *et seq.*;

y. N.J. Stat. Ann. § 56:8-163(a), *et seq.*;

z. N.C. Gen. Stat. Ann. § 75-65(a), *et seq.*;

aa. N.D. Cent. Code Ann. § 51-30-02, *et seq.*;

bb. Okla. Stat. Ann. Tit. 24 § 163(A), *et seq.*;

cc. Or. Rev. Stat. Ann. § 646A.604(1), *et seq.*;

dd. R.I. Gen. Laws Ann. § 11-49.3-4(a)(1), *et seq.*;

ee. S.C. Code Ann. § 39-1-90(A), *et seq.*;

ff. Tenn. Code Ann. § 47-18-2107(b), *et seq.*;

gg. Tex. Bus. & Com. Code Ann. § 521.053(b), *et seq.*;

hh. Utah Code Ann. § 13-44-202(1), *et seq.*;

ii. Va. Code. Ann. § 18.2-186.6(B), *et seq.*;

jj. Wash. Rev. Code Ann. § 19.255.010(1), *et seq.*;

kk. Wis. Stat. Ann. § 134.98(2), *et seq.*; and

ll. Wyo. Stat. Ann. § 40-12-502(a), *et seq.*

139. As a direct and proximate result of Mammoth's failure to reasonably safeguard the PII belonging to Plaintiff and class members, and Mammoth's failure to provide reasonable and timely notice of the Data Breach to Plaintiff and class members, Plaintiff and class members have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Mammoth's possession, and are entitled to damages in an amount to be proven at trial.

REQUEST FOR RELIEF

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

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

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

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

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

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

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

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

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

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

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

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

employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and class members;

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

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

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

m) Requiring Mammoth to implement logging and monitoring programs sufficient to track traffic to and from its servers; and

n) Requiring Mammoth to provide ten years of identity theft and fraud protection services to Plaintiff and class members.

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

4) For an award of statutory damages, as allowed by law in an amount to be determined;

5) For an award of punitive damages, as allowed by law in an amount to be determined;

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

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

8) For prejudgment interest on all amounts awarded; and

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

JURY DEMAND

Plaintiff, on behalf of himself and the Class of all others similarly situated, hereby demands a trial by jury on all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

Dated: June 1, 2020

Respectfully submitted,

/s/ Daniel L. Warshaw

Daniel L. Warshaw (CA Bar No. 185365)
PEARSON, SIMON & WARSHAW, LLP
15165 Ventura Boulevard, Suite 400
Sherman Oaks, CA 91403
Telephone: (818) 788-8300
Facsimile: (818) 788-8104
Email: dwarshaw@pswlaw.com

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

Hassan A. Zavareei (CA Bar No. 181547)
Mark A. Clifford*
TYCKO & ZAVAREEI LLP
1828 L Street NW, Suite 1000
Washington, D.C. 20036
Telephone: (202) 973-0900
Facsimile: (202) 973-0950
Email: hzavareei@tzlegal.com
mclifford@tzlegal.com
Counsel for Plaintiff and the Proposed Class
**pro hac vice application forthcoming*

Exhibit A

From: **Wishbone App Safety** <safety@wishbo.ne>
Date: Sat, May 23, 2020 at 2:44 AM
Subject: Action Recommended on Wishbone: Security Incident Involving Your Personal Information
To:

Notice of Data Breach

We're writing to let you know about a recent incident concerning your personal information on the Wishbone app.

What happened?
On May 20, 2020, our team became aware of a security issue where we believe an unauthorized individual may have had access to Wishbone's database through stolen credentials.

What information was involved?
After learning of the incident, we immediately began an investigation and found that some of the compromised data included usernames, emails, phone numbers, timezone/region, full name, bio, gender, hashed passwords and profile pictures. No financial or other sensitive information was involved in the incident.

What we're doing:
We value your privacy and deeply regret that this has happened. We immediately invalidated any current access methods to user information and updated keys accordingly. We also ensured that all employees or services which require access use cybersecurity approved multi-factor authentication or similar methods. Across the board, we are implementing stronger security and encryption of personal information to ensure the safety of all of our users' data. We anticipate providing notification to the relevant regulatory authorities shortly.

What you can do:
While we will continue to do our best to secure your account, we encourage you to reset your Wishbone password and to monitor your account for any suspicious activity. If you use the same or similar password for other services, we would recommend you change those passwords as well.

Other important information:
Maintaining the integrity of confidential information is extremely important to us. We are continuing to investigate this matter and will take all the necessary steps to prevent this from happening again.

For more information:
If you have any questions at all, please do not hesitate to reply to this email (safety@wishbo.ne).

Sincerely,
The Wishbone Team

ClassAction.org
