LEWIS BRISBOIS BISGAARD & SMITH LLP

Allen E. Sattler
888 SW Fifth Avenue, Suite 900
Portland, Oregon 97204-2025
Allen.Sattler@lewisbrisbois.com
Direct: 714.668.5572

August 17, 2020

VIA ELECTRONIC MAIL

Attorney General Bob Ferguson
Office of the Attorney General
1125 Washington St SE
PO Box 40100
Olympia, WA 98504-0100
Email: SecurityBreach@atg.wa.gov

Re: Notice of Data Security Incident

Dear Attorney General Ferguson:

We represent Mammoth Media, Inc. ("Mammoth Media") in connection with a recent data security incident described in greater detail below. Mammoth Media takes the security and privacy of the personal information within its control very seriously and has taken steps to prevent a similar incident from occurring in the future.

1. Nature of the Security Incident

Mammoth Media is a mobile application ("app") developer. Since its founding in 2015, Mammoth Media has developed and launched four apps, including Wishbone, a social polling app where users can create, vote in, and comment on polls featuring a side-by-side comparison of any two items, spanning from music artists, TV shows, fashion/beauty trends, to politics. Users can vote in polls anonymously and without registering for a Wishbone account. However, registration is required before a user can create or comment on polls.

On May 20, 2020, Mammoth Media became aware of a data security incident involving the unauthorized access to certain databases for the Wishbone app. Upon learning about the incident, Mammoth Media immediately launched an investigation and engaged incident response counsel and a digital forensics firm to assist in determining what happened and whether any personal information of Wishbone registered users was accessed or acquired by the unauthorized individual(s) during the incident.

On May 23, 2020, although the investigation was in its infancy, out of an abundance of caution and in the interest of transparency, Mammoth Media provided email notification to all Wishbone registered users informing them of the incident and the categories of information believed to have been involved in the incident. In addition to the email notification, Mammoth also provided website notice of the incident. The notification for registered users was published at http://notice.wishbone.io/, and the notification for the press was published at http://security.wishbone.io/. Copies of the email notification and the website notifications are enclosed herein.

At the time of the notification, Wishbone had approximately 10.6 million users of which roughly 9.38 are United States residents. The incident was limited to the information of Wishbone registered users and the information of users of Mammoth Media's other apps was not affected.

As the investigation progressed, Mammoth Media determined that a criminal group gained access to Wishbone registered users' information on January 27, 2020. In addition, it was able to confirm that the following categories of information were involved the incident: name, email address, hashed password, detected time zone/region, gender, bio, profile picture, and social media usernames. The affected information also includes the phone numbers of approximately 1 million registered users and birthdates of approximately 423,000 registered users. Accordingly, Mammoth Media is providing the instant notice to the Washington Office of the Attorney General as well as an updated website notice. A copy of the updated website notification is enclosed herein.

2. Number of Washington Residents Affected

Because Mammoth Media does not collect addresses as a part of its user registration process, it is unable to determine how many Washington residents have been affected by the incident. The incident involved the birthdates of approximately 423,000 registered users.

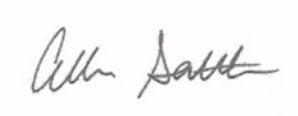
3. Measures Taken to Address the Incident

In response to the incident, Mammoth Media has taken steps to secure its environment and prevent a similar event from occurring in the future. Those measures include a global password reset for all registered users, adding another layer of security to encrypted registered user passwords, purging registered users' birthdates from its databases, the implementation of multi-factor authentication ("MFA") for the affected systems, and performing an audit of and updating access permissions on such systems.

4. Contact information

Mammoth Media is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information, please do not hesitate to contact me at 714-668-5572 or Allen.Sattler@lewisbrisbois.com.

Sincerely,



Allen E. Sattler of
LEWIS BRISBOIS BISGAARD & SMITH LLP

AES
Encl.: Notification Email
Website Notice – Registered Users
Website Notice – Press
Updated Website Notice – Registered Users

Action Recommended on Wishbone: Security Incident Involving Your Personal Information

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@getwishbo.ne).

Sincerely,
The Wishbone Team

wishbone

Updated Notice of Data Security Incident

Date: August 14, 2020

Dear Wishbone users,
This post is to provide updated information regarding the data security incident experienced by Mammoth Media, Inc. that involved the information of Wishbone registered users. Although the incident did not involve your Social Security number, government identification number, or financial account information, we are providing you with information regarding this incident and steps you can take to protect your personal data.

What happened?
On May 20, 2020, Mammoth Media became aware of a data security incident involving the unauthorized access to certain databases for the Wishbone app. Upon learning about the incident, we immediately launched an investigation and engaged an independent digital forensics firm to assist in determining what happened and whether any personal information of Wishbone registered users was accessed or acquired by the unauthorized individual(s) during the incident. Through the course of the investigation, Mammoth Media identified indicators that that a criminal group gained access to Wishbone users' information on January 27, 2020. We were also able to confirm the categories of information involved in the incident.

What information was involved?
If you registered for Wishbone prior to January 27, 2020, the following information may have been involved in this incident: your name, email address, hashed password, detected time zone/region, gender, bio, and profile picture. If you provided us with your phone number, date of birth, and social media

usernames, that information may have been involved as well.

What are we doing?
Mammoth Media took immediate actions to ensure that the unauthorized activity was not on-going and launched an investigation to determine the timeline, source, and scope of the incident. On May 23, 2020, although the investigation was in its infancy, out of an abundance of caution and in the interest of transparency, we provided email notification to all Wishbone registered users informing them of the incident and the categories of information believed to have been involved in the incident. In addition to the email notification, we published a notice about the incident here.

Mammoth Media also implemented additional measures to enhance the security of our digital environment. Furthermore, we are providing you with information about steps that you can take to help protect your personal information.

What can you do?
It is good practice to regularly change your passwords, including your password for Wishbone. It is also good practice to use complex passwords and not reuse the same password across multiple platforms, apps, or websites. If you have any questions or concerns about this incident, please email us at (safety@wishbo.ne). We are dedicated to protecting the privacy of our users' personal information and take this incident very seriously. We continue to implement additional security protocols across our business. We value our users' privacy and deeply regret that this has happened.
Sincerely, The Wishbone Team

Sincerely,
The Wishbone Team

Notice of Data Breach

Date: May 23, 2020

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 email us at (safety@wishbo.ne)

Sincerely,
The Wishbone Team

wishbone

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 email us at (safety@wishbo.ne)

Sincerely,
The Wishbone Team

wishbone

Press Notification

On May 20, 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. Personal information for some of our users was compromised. No financial or other sensitive information was involved. We have since invalidated any current access methods to user information and updated keys accordingly, and we've 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 value our users' privacy and deeply regret that this has happened.

Sincerely,
The Wishbone Team