Christopher J. DiIenno
Office: (267) 930-4775
Fax: (267) 930-4771
Email: cdiienno@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

June 10, 2020

VIA E-MAIL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-mail: securitybreach@atg.wa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent Zoosk, Inc. ("Zoosk") located at 3300 N. Ashton Blvd, Suite 240 Lehi, UT 84043, and are writing to notify your office of an incident that may affect the security of some personal information relating to Washington residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Zoosk does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

On May 11, 2020, Zoosk was alerted to a potential compromise of certain Zoosk user information. Zoosk immediately launched an investigation with the assistance of outside cybersecurity and forensic specialists and contacted law enforcement authorities. Zoosk is committed to providing its full cooperation with their investigative and prosecutorial activities. While the investigation remains ongoing, Zoosk determined that an unauthorized third party gained access to Zoosk data stored in a database hosted by a third party on or around January 12, 2020. The database contained certain information a user may have included in a user's online Zoosk profile, such as name, username (email address), date of birth, generalized demographical information, gender, and gender search preferences. While not confirmed, passwords may also have been affected. The database did not contain financial or credit card data. Zoosk does not collect Social Security numbers, driver's licenses, passport numbers, or other taxation or government identity information, so none of these types of information are at issue.

Pursuant to Wash. Rev. Code Ann. § 19.255.010 (West) the personal information that could have been subject to unauthorized acquisition includes name and date of birth. While unconfirmed at this time, a user's password for his/her Zoosk online account may have been subject to unauthorized access.

Notice to Washington Residents

On June 3, 2020, Zoosk began providing direct notice of this incident to all affected individuals by email, which includes 115,158 Washington residents. Please note, this number is a best estimate of impacted individuals for Washington. Zoosk maintains email address information for its members and not physical address information. Email notification is being provided in substantially the same form as the email draft attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Zoosk moved quickly to investigate and respond to the incident, assess the security of Zoosk systems, and notify potentially affected individuals. Zoosk implemented various remediation efforts such as changing and rotating passwords, changing access keys, enabling multifactor authentication, monitoring of user activity and access, and is assessing the implementation of additional safeguards and training to its employees.

In an abundance of caution, Zoosk is advising its members to change their password for their Zoosk account and is providing additional information on password security practices. Zoosk is also providing impacted individuals with guidance on how to better protect personal information, including advising individuals to report any suspected incidents of identity theft or fraud to law enforcement and information regarding security freezes and fraud alerts. Zoosk is providing the contact details for the national consumer reporting agencies and a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring credit reports. Zoosk established a dedicated call center to offer support to its members and to respond to member questions and concerns related to the event. Contact information for the Federal Trade Commission was also provided.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4775.

Very truly yours,

Christopher J. DiIenno of
MULLEN COUGHLIN LLC

CJD/gec

EXHIBIT A

Dear Zoosk Member,

We are writing to inform you of a recent data security event that may affect some of your personal information. We, at Zoosk, take the security of our community and the information in our care very seriously. On May 11, 2020, we learned that an unknown third party claimed to have accessed certain Zoosk member information. We immediately launched an investigation with the assistance of outside cybersecurity and forensic specialists. We also contacted law enforcement authorities and offered our full cooperation with their investigative and prosecutorial activities. Unfortunately, we learned during the course of these investigations that the information was authentic and related to certain Zoosk member information.

What happened and what data was affected?

While our investigation remains ongoing, we determined that an unauthorized third party gained access to Zoosk data stored in a database hosted by a third party on or around January 12, 2020. The database contained certain information you may have included in your online Zoosk profile, such as name, email address, date of birth, generalized demographical information, gender search preferences, and other profile information such as religious or political preferences. While not confirmed, passwords may also have been affected. The database did not contain financial or credit card data. Of course, as you know, we do not collect Social Security numbers, Social Insurance Numbers, driver's licenses, passport numbers, or other taxation or government identity information, so none of these types of information are at issue.

What steps has Zoosk taken?

In coordination with our outside specialists and with law enforcement authorities, we are taking several steps to monitor systems and enhance our existing security measures and processes. This is part of an ongoing process for any company and we are committed to improvement in this regard. We have also notified various regulatory authorities and continue to notify our affected members.

What should Zoosk members do?

We ask that you consider taking some protective measures as well. Out of an abundance of caution, we encourage you to change your Zoosk password. Regularly rotating online

passwords is a good security practice, as is avoiding the use of the same or similar passwords on multiple sites; consider selecting complex passwords with upper and lower case and special characters. You may also consider using a password generator from a trusted password tool. In addition, it is always a good idea to remain vigilant against threats of identity theft or fraud and to regularly review and monitor your accounts and credit history for any signs of unauthorized transactions or activity. If you ever suspect that you are the victim of identity theft or fraud, you have the right to file a report with the police or law enforcement. Finally, please be alert to “phishing” emails from someone who acts like they know you and requests sensitive information over email, such as passwords, financial information or government identification numbers (such as Social Security numbers or Social Insurance Numbers). We do not ask for this type of information over email.

Who do I contact for more information?

For questions related to this notice, please contact privacynotification@zoosk.com or call one of the phone numbers listed below. We appreciate the concern this may cause you. Please know that each member of the Zoosk community is important to us, and we are working tirelessly to respond to this event and protect the privacy and security of our users’ information.

Best regards,

Eric Eichmann
CEO of Spark Networks Group

Member Support Phone Numbers:
Hours of Operation

US & Canada:
1-866-289-6826
24 hours a day, 7 days per week

United Kingdom:
(+44) 0800 4584333
24 hours a day, 7 days per week

Germany:
(+49) 0800 1888946
24 hours a day, 7 days per week

France:
(+33) 0805104883
7:00a.m.-7:00p.m. CET, 7 days per week

Mexico:
(+52) 800 099 1172
7:00a.m.-7:00p.m. CDMX, 7 days per week

International:
(+44) 8000837779
24 hours a day, 7 days per week

To our United States members, we are required to provide the following as part of this message and we are happy to do so. Please see below for this information:

You can educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

- Contact for the US Consumer Reporting Agencies is as follows:
    - **Experian** - P.O. Box 9554 Allen, TX 75013; toll-free phone number: 1-888-397-3742
    - **TransUnion** - P.O. Box 2000 Chester, PA 19016: toll-free phone number: 1-800-916-8800
    - **Equifax** - P.O. Box 105069 Atlanta, GA 30348; toll-free phone number: 1-888-548-7878
- The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.
- *For Rhode Island residents,* the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.
- *For New York residents,* the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years.

This notice was not delayed by law enforcement.
