VIA U.S. MAIL

NH DEPT OF JUSTICE
JUL 14 2022 PM 12:35

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: **Notice of Data Event**

Dear Sir or Madam:

We write on behalf of Zola, Inc. ("Zola"), located at 7WTC, 250 Greenwich St., 39th Floor, New York NY 10007 and are writing to notify your office of an incident that may affect the security of information relating to 12 New Hampshire 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, Zola does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On May 21, 2022, Zola discovered suspicious activity occurring on its website and mobile application. Zola immediately secured and issued a forced password reset on user accounts and commenced an investigation to determine the scope of the incident and the information involved. Later on May 21, 2022 the investigation determined that an unknown actor had accessed certain users' login credentials from an unknown, external source and used those credentials to execute a credential stuffing attack against a limited number of Zola user accounts. The compromised credentials were not obtained from Zola systems.

Zola then carefully reviewed potentially impacted user accounts to determine what information may have been accessed by the unknown actor. On or about May 24, 2022, Zola confirmed the information involved includes: first and last name, address, phone number, and, in limited cases, incomplete payment card information. Importantly, individuals' full payment card and CVV numbers are not stored on Zola's systems and were not acquired as a result of the incident.

Notice to New Hampshire Residents

On or about July 5, 2022,Zola began providing written notice of this incident to all affected individuals, which includes 12 New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A.***

Other Steps Taken and To Be Taken

Upon discovering the event, Zola moved quickly to investigate and respond to the incident, assess the security of Zola accounts and systems, and notify potentially affected individuals. Zola is also working to implement additional safeguards and training to its employees.

Additionally, Zola is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Zola is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact

details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report any attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at legal@zola.com or (917) 410-6062.

Very truly yours,

Suzanne Lee
SVP, Legal

Exhibit A

[Please see attached.]

Zola, Inc.
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Credential Stuffing Incident

Dear <<Name 1>>:

We are writing to follow up with you about a recent credential stuffing incident involving your Zola account. Taking care of our couples is our top priority here at Zola, and we sincerely apologize for any stress or concern this incident may have caused you. We understand events like this can be unsettling, and because of this, we want to provide you with further information about what happened and the steps we have taken to protect your information.

WHAT HAPPENED?

On May 21, 2022, we detected unusual activity on our website and mobile application that prompted us to investigate immediately. Our investigation determined that, beginning on May 20, 2022, our website and mobile application had come under a form of attack known as "credential stuffing." Credential stuffing is when cyber attackers use email addresses/usernames and passwords stolen from another source, such as a breach of another website, to gain unauthorized access to user accounts. Based on our investigation, we believe that the cyber attacker in this incident previously gained access to the email address and password for your Zola account from another source (not from Zola). As a result, the unauthorized actor may have accessed certain information stored within, or may have conducted unauthorized activity on, your Zola account. Within hours of determining that a credential stuffing attack had occurred, our Trust & Safety Team decided, out of an abundance of caution, to reset passwords for all Zola registered users, regardless of whether suspicious activity was detected on their account. We have also reported the incident to law enforcement and worked to address or reverse any known unauthorized account activity.

WHAT INFORMATION WAS INVOLVED?

As described above, we believe that the cyber attacker obtained your email address and the password for your Zola account from another source. Using these credentials, the unauthorized actor may have accessed information stored on your account, such as your name, purchase history, shipping address, phone number and the amount of Zola store credit on your account (if any). If you saved your credit or debit card information or your bank account information to your Zola account, the unauthorized actor was able to view the partial information listed below.

- If you saved your payment card to your Zola account, the unauthorized actor was able to view the last four digits of your card number, the expiration date and the billing address. The unauthorized actor was *not* able to view your full card number or your CVV (the short code on the back of your card), because we do not store that information on Zola's systems.
- If you saved your bank account information to your Zola account, the unauthorized actor was able to view the last four digits of your bank account number and the name of your bank. The unauthorized actor was *not* able to view your full bank account number, routing number or date of birth, because we do not store this information on Zola's systems.

WHAT WE ARE DOING

Zola values your privacy and deeply regrets that this incident occurred. As soon as we found out about the unusual activity, we began working around the clock to protect our couples, swiftly investigating the incident, immediately notifying our community and resetting passwords for all Zola registered users. We are engaged in a continual process to enhance our security measures, including working with an external security company in addition to our internal Trust & Safety Team to protect our community.

WHAT YOU CAN DO

As described above, we have already reset your password, which you can change at https://www.zola.com/account/forgot-password. We urge you to choose a password that is strong and unique to Zola. If you used your previous password on other sites we highly recommend you also change your password on those sites. While we have no reason to believe that any further unauthorized use of your information will occur as a result of this incident, credential stuffing attacks are increasingly common, and we always encourage you to remain vigilant in monitoring your account statements and credit reports for unauthorized activity. If you ever notice any unusual activity on your Zola account, please reach out to us at firstresponse@zola.com. Please also review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on steps you can take to protect your information.

FOR MORE INFORMATION

For further information and assistance, please contact our team any time at firstresponse@zola.com, call (866) 657-5392 seven days a week, 10 AM - 6 PM EST or write to us at Zola, Inc., 7WTC, 250 Greenwich St., 39th Floor, New York, NY 10007.

Sincerely,

The Zola Team

Steps You Can Take to Further Protect Your Information

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus: Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-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. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact any of the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 441 4th St. NW #1100, Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Zola, Inc. is located at 7WTC, 250 Greenwich St., 39th Floor, New York, NY 10007.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are <<#>> Rhode Island residents impacted by this incident.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.