EXHIBIT 1

This notice is intended to make your office aware of an incident that may affect the security of certain personal information of approximately 3,368 California residents. By providing this notice, ShopStyle does not waive any rights or defenses regarding the applicability of California law, the applicability of the California data incident notification statute, or personal jurisdiction. The investigation into this event is ongoing and this notice will be supplemented with any substantive facts learned subsequent to its submission.

Nature of the Data Event

On July 5, 2018, ShopStyle discovered unauthorized activity in one of its systems. ShopStyle immediately commenced an investigation to determine the nature and scope of the activity and the data contained in the relevant system. This investigation included working with a third party forensic investigator. Through the investigation, it was determined that a key was exposed permitting potential unauthorized access to certain ShopStyle data between April 16 - 27, 2018. ShopStyle, with the assistance of a third-party forensic investigator, conducted a thorough review of the available forensic artifacts and determined that it was unable to conclusively rule out access to data on the relevant system. ShopStyle then worked diligently to conduct a programmatic and manual review of the data to determine what data was present on the system and to whom it related. Through this review, ShopStyle determined that certain ShopStyle account holder email addresses/usernames and hashed passwords were stored in the impacted system. To date, ShopStyle has no evidence to suggest the user information was subject to attempted or actual misuse; however, in an abundance of caution, ShopStyle provided notice to potentially affected individuals.

Notice to California Residents

While the investigation in this incident is ongoing, on October 24, 2018, ShopStyle provided notice of this incident to those potentially impacted California residents. This notice will be provided in substantially the same form as the communication attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon learning of this incident, ShopStyle immediately rotated all corporate access keys and credentials of the impacted systems. ShopStyle audited reviewed its internal security procedures. ShopStyle will also be implementing a user password reset for those accounts potentially affected by this incident.

Additionally, while to date, the investigation has found no evidence of actual or attempted misuse of personal information potentially affected by this event, in an abundance of caution, ShopStyle is providing potentially impacted individuals with notice of this event. This notice informs the users that their passwords have been reset, that they are required to change their password, and encourages them to take other steps to protect their accounts for any other online accounts sharing their ShopStyle credentials. It also provide the potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, 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 attempted or actual identity theft and fraud. ShopStyle will also be providing notice of this event to other state regulators as required by law.

EXHIBIT A

Notice of Data Breach

ShopStyle Inc. ("ShopStyle") is writing to inform you about a recent incident that involved your account information.

What Happened? On July 5, 2018, we discovered that, between April 16 - 27, 2018, an unauthorized third party gained access to account credentials and accessed certain user information. Although we are unaware of any actual or attempted misuse of your information, we are providing you this notification out of an abundance of caution because your information was present in the system affected by this incident.

What Information Was Involved? Our investigation confirmed the information impacted may include your name (if provided), email address, and password. While we store all passwords in a protected format, we have reset your password out of caution.

What Are We Doing. Information privacy and security are among our highest priorities. We made improvements to our internal security procedures and are working with applicable regulatory authorities about this matter. We are also notifying potentially affected individuals, including you, so that you may take further steps to better protect your personal information, should you feel it is appropriate to do so.

What Can You Do. Although we are not aware of any actual or attempted misuse of information as a result of this event, we recommend you change your password or take other steps to protect your accounts for any other online accounts sharing your ShopStyle credentials. You may also review the information contained in the attached "Steps You Can Take to Protect Your Information."

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please write to us at help@shopstylecollective.com or at privacy@shopstyle.com.

We sincerely regret any inconvenience this incident may cause you. ShopStyle remains committed to safeguarding information in our care and we will continue to take proactive steps to enhance the security of our systems.

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity and to detect errors. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

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. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

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. Should you wish to place a fraud alert, please contact any one of the agencies listed above.

You can further 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.

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); 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 Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

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, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 33 Rhode Island residents impacted by this incident.