EXHIBIT 1

The investigation involving this incident is ongoing and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Arbonne does not waive any rights or defenses regarding the applicability of California law, the applicability of the California data event notification statute, or personal jurisdiction.

Nature of the Data Event

On the evening of April 20, 2020, Arbonne became aware of unusual activity within a limited number of its internal systems. Arbonne immediately commenced an investigation with the assistance of third-party computer specialists. While the investigation remains ongoing, the preliminary investigation determined that certain information in Arbonne's systems may have been accessed without authorization. On April 23, 2020, the investigation identified a data table containing limited personal information that may have been accessible to unauthorized actor.

Arbonne confirmed that the information that could have been subject to unauthorized access includes personal information as defined by Cal. Civ. Code § 1798.82(h)(2) such as name, address, username and password.

Notice to California Residents

On April 24, 2020, Arbonne provided preliminary notice to affected individuals and began providing supplemental written notice on May 22, 2020. The population of affected individuals includes three thousand five hundred twenty-seven (3,527) California 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, Arbonne moved quickly to investigate and respond to the incident, assess the security of Arbonne systems, and notify potentially affected individuals. Specifically, Arbonne forced a password reset for all user accounts whose passwords may have been subject to unauthorized access. As part of Arbonne's ongoing commitment to the security of information, Arbonne is also reviewing and enhancing existing policies and procedures. Arbonne is providing access to credit monitoring and identity protection services for one year through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Arbonne 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. Arbonne is providing individuals with 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. Arbonne has also reported this matter to the FBI and relevant regulators.

EXHIBIT A

[Name]
[Address]
[City, State, Zip] [Date]

Re: Notice of Data Breach

Dear [Name of Affected Individual]:

As a follow up to our preliminary notification on April 24, 2020, Arbonne International, LLC ("Arbonne") is writing to provide additional details on an incident that may affect the security of some of your personal information. While there is currently no evidence that your information has been misused as a result of this incident, out of an abundance of caution, we are providing you with additional information about the incident, our response, and resources available to you to better protect your information should you feel it appropriate to do so.

What Happened? On the evening of April 20, 2020, Arbonne became aware of unusual activity within a limited number of its internal systems. We immediately commenced an investigation with the assistance of third-party computer specialists. While the investigation remains ongoing, the preliminary investigation determined that certain information in Arbonne's systems may have been accessed without authorization. On April 23, 2020, the investigation identified a data table containing limited personal information that may have been accessible to unauthorized actor. Through this process, we determined that your personal information was present in the involved table. To date, we are not aware of any actual or attempted misuse of your personal information in relation to this incident.

What Information Was Involved? The ongoing investigation determined that the following types of your personal information were present in the table that may have been accessible by an unauthorized actor: your name, email and mailing addresses, order purchase history, phone number, and Arbonne account password. To date, our investigation has not determined that payment card information or government ID information, such as Social Security numbers, were accessed.

What We Are Doing. Arbonne takes the confidentiality, privacy, and security of information in its care very seriously. Upon learning of this incident, we promptly began an investigation to confirm the security of our systems. While our investigation is ongoing, in an abundance of caution, we forced a password reset for all users whose passwords may have been subject to unauthorized access and we notified these users to ensure they were aware of this incident.

While Arbonne has security measures in place to protect information in its care, we are also taking steps to enhance our data security; these steps include implementing additional safeguards, reviewing Arbonne policies and procedures, and additional employee training.

As an added precaution, Arbonne is providing you with access to twelve months of identity monitoring services from Kroll at no cost to you. A description of services and instructions on how to enroll can be found within the

enclosed Steps You Can Take to Help Protect Personal Information. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

What You Can Do. You can review the enclosed *Steps You Can Take to Protect Personal Information*. You can also enroll to receive the free identity monitoring services through Kroll.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have questions or concerns, please call Arbonne Customer Service 800-ARBONNE, Monday through Friday, 7am – 8pm Pacific excluding national holidays, or email us at securityinfo@custhelp.com

Sincerely,

Arbonne Data Privacy Officer

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring and Identity Theft Restoration Services

1. You must activate your identity monitoring services by << Enter Activation Deadline>>. Your Activation Code will not work after this date.
2. Visit https://enroll.idheadquarters.com/redeem to activate your identity monitoring services.
3. Provide Your Activation Code: <<Enter Activation Code>> and Your Verification ID: <<Enter Verification ID>>
4. To sign in to your account after you have activated your identity monitoring services, please visit https://login.idheadquarters.com/

Monitor Your Accounts

In addition to enrolling in the complimentary services detailed above, 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
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
P.O. 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.

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 below:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Additional Information

arbonne®

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. 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, 1-410-528-8662, www.oag.state.md.us.

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/.

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 agencies 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 North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

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. There are fifty-six (56) Rhode Island residents impacted by this incident.

arbonne®

Kroll | A Division of DUFF & PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.