

August 14, 2023

Office of the Attorney General
Attn: Security Breach Notification
Idtheft@oag.state.md.us

Dear Sir/Madam:

We are outside counsel to Shoyeido USA, Inc. (“Shoyeido”) and are contacting you on its behalf. Pursuant to Section 14-3504 of the Maryland Code, Commercial Law (“Law”), we are writing to notify you of a data security incident that may have allowed a third party unauthorized access to personal information involving residents of the State of Maryland.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

Shoyeido is a provider of incense products and sells its products online. Shoyeido uses an e-commerce service provider, CommerceV3, Inc. (“CommerceV3”) to help process payment card information when an order is placed on Shoyeido’s website. On June 6, 2023, CommerceV3 notified Shoyeido that CommerceV3 learned that an unauthorized party obtained access to CommerceV3’s systems. On July 11, 2023, CommerceV3 confirmed a threat actor installed a skimmer program on CommerceV3’s webserver, which possibly allowed the threat actor to access and/or acquire the personal information of Shoyeido’s customers during the time period between November 24, 2021 and December 13, 2022.

DATA INVOLVED

According to CommerceV3, the data that may have been exposed during the November 24, 2021 to December 13, 2022 time period includes the following information: name, email address, billing address, and payment card number along with the card’s CVV code and expiration date.

It is important to note that the data that was accessible did not include national insurance numbers, social security numbers, ID numbers, or any medical information.

STEPS TAKEN RELATING TO THE INCIDENT

Upon receipt of the June 6, 2023 notice, Shoyeido immediately launched an investigation into the matter and conducted a review of CommerceV3’s response to the incident. CommerceV3 confirmed that it has performed a forensic analysis of the attack and notified all major credit card brands about the suspected activity and the range of the suspected activity. Additionally, CommerceV3 confirmed that it removed the vulnerability and implemented additional security

Location

1800 Broadway, Suite 300
Boulder, CO 80302

Contact

p: 303.473.2700 | f: 303.473.2720
www.hollandhart.com

measures designed to prevent a recurrence of such an attack and to protect the privacy of all of its customers. Further, CommerceV3 confirmed that it has been in contact with law enforcement regarding the matter. In addition to receiving the foregoing assurances from CommerceV3, Shoyeido has independently contacted law enforcement and is working with law enforcement in their investigation of the security incident.

In accordance with the Law, Shoyeido will send notification via secure e-mail to the affected residents on or about August 14, 2023, in substantially the same form as the letter attached hereto.

Additionally, in accordance with the Law, Shoyeido hereby provides notice that 41 residents of Maryland were affected.

EXPLANATION FOR DELAY OF NOTIFICATION

There was a brief delay in providing notification, as Shoyeido had to work with CommerceV3 to understand more about the security incident and Shoyeido's reporting obligations. While Shoyeido was first alerted of the security incident on June 6, 2023 via CommerceV3, it was not able to confirm material facts about the security incident with CommerceV3 until July 11, 2023, including obtaining a timeline of the events, determining whether the data was encrypted, determining whether the data may have misused, and understanding what remedial actions CommerceV3 had taken. Once Shoyeido received the additional information it started to immediately prepare and take actions to determine and fulfill any notification obligations.

OTHER NOTIFICATION AND CONTACT INFORMATION

If you have any questions regarding this incident or if you desire further information or assistance, please call the undersigned at 303-473-4808 or contact Alex Kimata at 303-441-5906.

Sincerely,

Richard D. Spilde

Richard D. Spilde, Jr., P.C.
Partner
of Holland & Hart LLP

Enclosure: Sample Breach Notification Letter

cc: Shoyeido

NOTICE OF DATA BREACH

Confidential-for Intended Recipient Only

Click or tap to enter a date.

Dear Click or tap here to enter text.,

Shoyeido USA, Inc. (“Shoyeido”) values your business and respects the privacy of your information, which is why we are writing to notify you about a data security incident that may have involved your personal information. We recommend that you closely review the information provided in this notice for suggestions on how to protect yourself against potential misuse of your information.

1. What Happened?

Shoyeido uses an e-commerce service provider, CommerceV3, Inc. (“CommerceV3”) to help process payment card information when an order is placed on Shoyeido’s website. On June 6, 2023, CommerceV3 notified Shoyeido that CommerceV3 learned that an unauthorized party obtained access to CommerceV3’s systems. On July 11, 2023, CommerceV3 confirmed a threat actor installed a skimmer program on CommerceV3’s webserver, which possibly allowed the threat actor to access and/or acquire the personal information of Shoyeido’s customers during the time period between November 24, 2021 and December 13, 2022.

2. What Data Was Involved?

According to CommerceV3, the data that may have been exposed during the November 24, 2021 to December 13, 2022 time period includes the following information: name, email address, billing address, and payment card number along with the card’s CVV code and expiration date.

It is important to note that the data that was accessible did not include national insurance numbers, social security numbers, identification numbers, or any medical information.

3. What Are The Potential Consequences For You?

It cannot be ruled out that the data mentioned above may be misused and that you may have unauthorized charges on any payment card you used with us. Further, it cannot be guaranteed that the accessible information will not be used to contact you or further advertise to you.

4. What We Are Doing.

Upon receipt of the June 6, 2023 notice, Shoyeido immediately launched an investigation into the matter and conducted a review of CommerceV3’s response to the incident. CommerceV3 confirmed that it has performed a forensic analysis of the attack and notified all major credit card brands about the suspected activity and the range of the suspected activity. Additionally, CommerceV3 confirmed that it removed the vulnerability and implemented additional security measures designed to prevent a recurrence of such an attack and to protect the privacy of all of its customers. Further, CommerceV3 confirmed that it has been in contact with law enforcement regarding the matter. In addition to receiving the foregoing assurances from CommerceV3, Shoyeido has independently contacted law enforcement and is working with law enforcement in their investigation of the security incident.

5. What You Can Do.

Please review the attachment to this letter (Further Information for You) for additional information on how to protect against identity theft and fraud, including services about fraud alerts and security freezes. We encourage you to remain vigilant against incidents of fraud or identity theft by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. If you find any suspicious activity, you should immediately report such activity to law enforcement, including the Attorney General office where you live or, the Federal Trade Commission.

6. For More Information.

Please call us at 1-800-786-5476 if you have any questions.

We truly apologize for this incident and regret any inconvenience to our customers.

Sincerely,

Shoyeido USA, Inc. Executive Team

Further Information for You

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®
P.O. Box 740241
Atlanta, GA 30374-0241
1-866-349-5191
www.equifax.com

Experian®
P.O. Box 2002
Allen, TX 75013-9701
1-866-200-6020
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-888-4213
www.transunion.com

You should remain vigilant for incidents of fraud or identity theft by reviewing account statements and monitoring free credit reports. When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information about you by consumer reporting agencies. For more information about your rights under the FCRA, please visit https://www.ftc.gov/system/files/ftc_gov/pdf/fcra-may2023-508.pdf or www.ftc.gov.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax®
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045
www.equifax.com/personal/credit-report-services

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

TransUnion®
P.O. Box 160
Woodlyn, PA 19094
1-800-916-8800
www.transunion.com/credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

- Full name, with middle initial and any suffixes;
- Social Security number;
- Date of birth (month, day, and year);
- Current address and previous addresses for the past five (5) years;
- Proof of current address, such as a current utility bill or telephone bill; and
- Other personal information as required by the applicable credit reporting agency.

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts one (1) year and 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 (7) years. Should you wish to place a fraud alert, please contact any one of the agencies listed below.

The agency you contact will then contact the other two credit agencies.

Equifax®
P.O. Box 105069
Atlanta, GA 30348-5069
1-800-525-6285
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

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

TransUnion®
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
www.transunion.com/fraud-alerts

Federal Trade Commission and State Attorneys General Offices

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact local law enforcement, the Federal Trade Commission and/or the Attorney General's office in your home state. If you are a **District of Columbia resident**, you may contact the Office of the Attorney General for the District of Columbia, Consumer Protection Division, at 400 6th Street, NW, Washington, DC 20001, (202) 727-3400, <https://oag.dc.gov/about-oag/contact-us>. If you are a **Maryland resident**, you may contact the Maryland Office of the Attorney General at Consumer Protection Division Office, 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, <https://www.marylandattorneygeneral.gov/Pages/contactus.aspx>, 1-888-743-0023, or 410-528-8662 (consumer). If you are a **New York resident**, you may contact the Office of the New York State Attorney General, The Capitol Albany NY 12224-0341, <https://ag.ny.gov/contact-attorney-general-letitia-james>, 1-800-771-7755. If you are a **North Carolina resident**, you may contact the North Carolina Office of the Attorney General at Consumer Protection, 9001 Mail Service Center Raleigh, NC 27699-9001, <https://ncdoj.gov/contact-doj/>, (877) 566-7226, or (919) 716-6000. If you are a **Rhode Island resident**, you may contact the Rhode Island Attorney General at 150 South Main Street, Providence, RI 02903; <https://riag.ri.gov/about-our-office/contact-us>; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft, including the use of fraud alerts and security freezes. You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).