

# VEDDER PRICE.

BRUCE A. RADKE  
SHAREHOLDER  
+1 (312) 609 7689  
bradke@vedderprice.com

222 NORTH LASALLE STREET  
CHICAGO, ILLINOIS 60601  
T: +1 (312) 609 7500  
F: +1 (312) 609 5005

CHICAGO • NEW YORK • WASHINGTON, DC  
LONDON • SAN FRANCISCO • LOS ANGELES

May 27, 2016

**VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US) AND  
FEDERAL EXPRESS**

Office of the Attorney General  
Attn: Jeff Karberg, Administrator of the Identity Theft Program  
Attn: Security Breach Notification  
200 St. Paul Place  
Baltimore, MD 21202

***Re: Notification of a Computer Security Incident Involving Personal Information***

Dear Mr. Karberg:

This follows on my voicemail to you on May 27, 2016. As I explained, we represent Ben Bridge Jeweler, Inc. ("Ben Bridge") in connection with a recent incident that may have impacted the security of certain personal information of one (1) Maryland resident. Ben Bridge is reporting an unauthorized access of unencrypted computerized data containing personal information pursuant to Md. Code Ann., Com. Law § 14-3504(h).

The investigation of this incident is ongoing, and this notice will be supplemented, if necessary, with any significant new facts discovered subsequent to its submission. By providing this notice, Ben Bridge does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction in connection with this incident.

**Background of the Incident**

Ben Bridge (www.benbridge.com) was founded in Seattle, Washington in 1912 on a simple promise: to offer the finest jewelry, best selection and friendly, knowledgeable service. Family-run for five generations, Ben Bridge operates more than eighty (80) retail stores in eleven (11) states including Alaska, Arizona, California, Colorado, Hawaii, Minnesota, Nevada, New Mexico, Oregon, Texas and Washington.

# VEDDER PRICE

Office of the Attorney General

May 27, 2016

Page 2

On Wednesday, May 18, 2016, Ben Bridge was the target of an e-mail phishing attack that resulted in the disclosure of certain of its current and former employees' 2015 W-2 forms, including those employees' first and last names, addresses, Social Security numbers and compensation information. Upon discovering the incident, Ben Bridge promptly launched an internal investigation and notified the Federal Bureau of Investigation ("FBI") and the Internal Revenue Service ("IRS"). Ben Bridge is cooperating in the FBI's and IRS's investigations into this incident.

## **Notice to the Maryland Resident**

On May 25, 2016, Ben Bridge provided notice of the incident via e-mail to its affected employees, including the Maryland resident. On May 27, 2016, Ben Bridge will be sending a further written notification letter to the affected Maryland resident. Attached is a sample of the notification letter that is being sent to the affected Maryland resident via first-class United States mail.

Ben Bridge has also arranged to offer two (2) years of complimentary credit monitoring and identity theft protection services through Experian to the affected Maryland resident.

In addition, Ben Bridge has established a confidential inquiry line (888-774-3252) that the affected Maryland resident can contact between 6:00 a.m. and 6:00 p.m., Pacific time, Monday through Friday, to ask questions and to receive further information regarding the incident.

## **Other Steps Undertaken and to Be Undertaken by Ben Bridge**

Ben Bridge has already begun taking several actions to help prevent this type of incident from occurring in the future. These actions include evaluating ways to best strengthen Ben Bridge's systems to guard against similar attacks in the future and reminding its employees of the risks of phishing attacks and providing them with additional information on best practice for cybersecurity. At the IRS's request, Ben Bridge will be providing the Social Security numbers of the impacted current and former employees, including the Maryland resident, so that the IRS can identify potential suspicious tax returns related to the 2015 tax year that may be filed using those employees' Social Security numbers.

VEDDER PRICE

Office of the Attorney General

May 27, 2016

Page 3

**Contact Information**

Please contact me if you have any questions or if I can provide you with any further information concerning this matter. Thank you.

Very truly yours,



Bruce A. Radke

BAR/bah

Enclosure

cc: Ed Bridge, co-Chief Executive Officer and President, Ben Bridge Jeweler, Inc.  
Jon Bridge, co-Chief Executive Officer and General Counsel, Ben Bridge Jeweler, Inc.



Return Mail Processing Center  
PO Box 6336  
Portland, OR 97228-6336

<<Name>>  
<<Address>>  
<<Address>>  
<<City>>, <<State>> <<Zip>>

<<Date>>

Dear <<Name>>:

Ben Bridge Jeweler, Inc. recently discovered that we were the target of a criminal cyber attack that impacted certain of your personal information. We value and respect your privacy, which is why we are writing to advise you of the steps that Ben Bridge has undertaken since discovering the incident and to provide you with information on what you can do to better protect yourself, should you feel it is appropriate to do so.

As to the incident itself, on May 18, 2016, a phishing attack directed at Ben Bridge resulted in the disclosure of certain of our employees' IRS Form W-2s, Wage and Tax Statements, including your first and last name, address, Social Security number and compensation information. Upon discovering the incident, Ben Bridge promptly notified the Federal Bureau of Investigation and the Criminal Investigation Division of the Internal Revenue Service.

Ben Bridge is offering you two years of free credit monitoring and identity protection services through Experian's® ProtectMyID® Alert, which will promptly alert you to potential issues and help you resolve them. ProtectMyID® Alert is being offered at no cost to you. Please see the additional information below for instructions on how to activate your complimentary two-year ProtectMyID® Alert membership using the Activation Code listed below.

We have already begun taking several actions to help prevent this type of incident from occurring in the future. These actions include evaluating ways to best strengthen our systems to guard against similar attacks in the future and reminding employees of the risks of phishing attacks and providing them with additional information on best practices for cybersecurity. At the IRS's request, Ben Bridge is providing your Social Security number to the IRS. This will allow the IRS to identify any potential suspicious future tax returns related to the 2015 tax year that may be filed using your Social Security number.

Additionally, we have established a confidential inquiry line to assist you with any questions regarding this incident. This confidential inquiry line is available between 6 a.m. and 6 p.m., Pacific time, Monday through Friday, at 888-774-3252.

We value the trust you place in Ben Bridge to protect the privacy and security of your personal information, and we apologize for any inconvenience or concern that this incident might cause you.

Sincerely,

*Ed Bridge*

Ed Bridge, co-Chief Executive Officer and President

*Jon Bridge*

Jon Bridge, co-Chief Executive Officer and General Counsel

## Activating Your Complimentary Credit Monitoring

To help protect your identity, we are offering a **complimentary** two-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

### Activate ProtectMyID Now in Three Easy Steps

1. **ENSURE** that you enroll by <<Enroll Date>>. (Your code will not work after this date.)
2. **VISIT** the ProtectMyID Website to enroll: [www.protectmyid.com/redeem](http://www.protectmyid.com/redeem).
3. **PROVIDE** your Activation Code: <<ACTIVATION\_CODE>>.

If you have questions or need an alternative to enrolling online, please call 1-877-288-8057 and provide engagement #<<Engagement PC #>>.

### ADDITIONAL DETAILS REGARDING YOUR TWO-YEAR PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free Copy of your Experian Credit Report**
- **Surveillance Alerts for the following:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes and suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution and ProtectMyID ExtendCARE:** Toll-free access to U.S.-based customer care and a dedicated Identity Theft Resolution Agent who will walk you through the process of fraud resolution from start to finish for seamless service. The agent will investigate each incident; help you contact credit grantors to dispute charges and close accounts, including credit, debit and medical insurance cards; assist with freezing credit files; and contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance\*:** Immediately covers certain costs, including lost wages, private investigator fees and unauthorized electronic fund transfers.

**Activate your membership today at [www.protectmyid.com/redeem](http://www.protectmyid.com/redeem) or call 1-877-288-8057 to register with the activation code above.**

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 1-877-288-8057.

\* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and is intended for informational purposes only, and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions and exclusions of coverage. Coverage may not be available in all jurisdictions.

## Additional Important Information

In the aftermath of similar incidents, some opportunistic criminals seek to fraudulently obtain personal information of affected individuals by claiming to be the business experiencing the breach. Please be extremely cautious when giving out personal information and do **not** disclose your Social Security number via e-mail (including to us). Do **not** respond to any e-mail requests from entities requesting your Social Security number, date of birth, financial account numbers, login/password information or other sensitive personal information. We will not ask you for your Social Security number, date of birth, financial account number or other sensitive personal information with regard to this incident. If you receive any written request or electronic request via e-mail purporting to be from Ben Bridge Jeweler, Inc., and it looks suspicious, please notify us immediately. The IRS does **not** initiate contact with taxpayers by e-mail, fax or any social media tools to request personal financial information. If you receive an e-mail or similar request that appears to be from the IRS, the IRS suggests that you do not respond to any such requests. If you become aware that a false tax return has been filed with your name and social security number, in addition to taking the appropriate steps outlined by the IRS on their website, please notify us via email at [notification@benbridge.com](mailto:notification@benbridge.com).

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your credit card account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You can also complete and submit IRS Form 14039, Identity Theft Affidavit which can be found at [irs.gov/pub/irs-pdf/f14039.pdf](http://irs.gov/pub/irs-pdf/f14039.pdf). You can mail or fax the completed form to the IRS instructions included on the form. Additionally, the IRS offers further guidance for protecting your identity at the following website: <https://www.irs.gov/individuals/identity-protection>. There are a number of tools listed there that may be helpful you.

Additionally, you may want to consider reviewing your social media sites, such as Facebook, to avoid inadvertently disclosing your sensitive personal information such as your date of birth. You may also want to consider filing a report with your local police.

**Credit Reports:** You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting <http://www.annualcreditreport.com>, by calling toll free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at: <https://www.annualcreditreport.com/cra/requestformfinal.pdf>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files, is as follows:

Equifax  
1-800-349-9960  
[www.equifax.com](http://www.equifax.com)  
P.O. Box 105788  
Atlanta, GA 313048

Experian  
1-888-397-3742  
[www.experian.com](http://www.experian.com)  
P.O. Box 9554  
Allen, TX 75013

TransUnion  
1-888-909-8872  
[www.transunion.com](http://www.transunion.com)  
P.O. Box 2000  
Chester, PA 19022

**Fraud Alerts:** You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that creditors contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at <http://www.annualcreditreport.com>.

**Credit and Security Freezes:** You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number 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 on your credit file, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may cause a delay should you attempt to obtain credit. In addition, you may incur fees for placing, lifting and/or removing a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze  
P.O. Box 105788  
Atlanta, GA 30348

Experian Security Freeze  
P.O. Box 9554  
Allen, TX 75013

TransUnion Security Freeze  
Fraud Victim Assistance Department  
P.O. Box 6790  
Fullerton, CA 92834

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

**Maryland Residents:** Maryland residents can contact the Office of the Attorney General at:

Office of the Attorney General  
220 St. Paul Place  
Baltimore, MD 21202  
(888) 743-0023  
[www.oag.state.md.us](http://www.oag.state.md.us)

**North Carolina Residents:** North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at:

North Carolina Attorney General's Office  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
(877) 566-7226  
[www.ncdoj.com](http://www.ncdoj.com)