BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Craig A. Hoffman
direct dial: 513.929.3491
cahoffman@bakerlaw.com

October 12, 2016

VIA E-MAIL (CONSUMER@IOWA.GOV) AND OVERNIGHT MAIL

Iowa Attorney General
Consumer Protection Division
1305 E. Walnut Street
Des Moines, IA 50319

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client, Vera Bradley, to notify you of a security incident that may have involved the payment card information of Iowa residents.

On September 15, 2016, Vera Bradley was provided information from law enforcement regarding a potential data security issue related to its retail store network. Vera Bradley responded by immediately notifying the payment card networks and initiating an investigation with the assistance of a leading computer security firm to gather facts and determine the scope of the issue. Findings from the investigation show unauthorized access to Vera Bradley's payment processing system and the installation of a program that looked for payment card data.

The program was specifically designed to find track data from the magnetic stripe of a payment card as the data was being routed through the affected payment systems. Track data in the magnetic stripe of a payment card may contain the card number, cardholder name, expiration date, and internal verification code.

Some, but not all, payment cards used at Vera Bradley retail store locations between July 25, 2016 and September 23, 2016 may have been affected. Cards used on Vera Bradley's website were not affected.

Vera Bradley has taken significant steps to stop the attack and strengthen the security of its network environment, including resetting all enterprise passwords, blocking certain network communication attempts, and removing affected systems from the network. Since the payment

card networks have been notified, they can work with the banks that issued payment cards used during the affected time period. Lastly, Vera Bradley has established a dedicated call center that potentially affected individuals can call with questions regarding the incident.

Vera Bradley is not able to identify the total number of potentially affected Iowa residents, and Vera Bradley cannot identify a name and mailing address for most potentially affected residents. Thus, pursuant to Iowa Code Ann. §715C.2, Vera Bradley is providing substitute notification today to Iowa residents who used their payment cards at an affected Vera Bradley retail location during that location's affected time frame by posting a statement on its website, issuing a press release, and sending an email (to those individuals for whom Vera Bradley has an email address). The substitute notification, press release and email notice are enclosed. Vera Bradley has been able to identify the mailing address of 101 Iowa residents who used their payment cards at an affected Vera Bradley retail location. In accordance with Iowa Code Ann. §715C.2, Vera Bradley will be mailing a letter to these individuals. A copy of the notification letter is enclosed. Notification is being provided without unreasonable delay following the completion of an investigation by Vera Bradley to determine the scope of the incident. *See* Iowa Code Ann. §715C.2.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Craig A. Hoffman
Partner

Enclosures

Vera Bradley Notifies Customers of Payment Card Incident
October 12, 2016

California residents please click here

On September 15, 2016, Vera Bradley was provided information from law enforcement regarding a potential data security issue related to our retail store network. Upon learning this information, we immediately notified the payment card networks and initiated an investigation with the assistance of a leading computer security firm to aggressively gather facts and determine the scope of the issue.

Payment cards used at Vera Bradley retail store locations between July 25, 2016 and September 23, 2016 may have been affected. Not all cards used during this time frame were affected. Cards used on our website have not been affected.

Findings from the investigation show unauthorized access to Vera Bradley's payment processing system and the installation of a program that looked for payment card data. The program was specifically designed to find track data in the magnetic stripe of a payment card that may contain the card number, cardholder name, expiration date, and internal verification code - as the data was being routed through the affected payment systems. There is no indication that other customer information was at risk.

It is always advisable to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to your card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the section that follows this notice for additional steps you may take to protect your information.

Vera Bradley has stopped this incident, and we continue to work with the computer security firm to further strengthen the security of our systems to help prevent this from happening again.

Vera Bradley values the relationship we have with our customers and understands the importance of protecting personal information. We regret any inconvenience this may have caused. If you have questions, please call 844-723-9340 from 9:00 a.m. to 9:00 p.m. EDT, Monday to Friday.

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2002, Allen, TX 75013, www.experian.com,1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit 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, 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 delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove 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.

If you are a resident of Maryland, North Carolina, or Rhode Island, you may contact and obtain information from your state attorney general at:

- *Maryland Attorney General's Office,* 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023 (toll free when calling within Maryland)
- (410) 576-6300 (for calls originating outside Maryland)
- *North Carolina Attorney General's Office,* 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400
- *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400

If you are a resident of Massachusetts, note that pursuant to Massachusetts law, you have the right to file and obtain a copy of any police report.

Massachusetts law also allows consumers to request a security freeze. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services.

The fee for placing a security freeze on a credit report is $5.00. If you are a victim of identity theft and submit a valid investigative report or complaint with a law enforcement agency, the fee will be waived. In all other instances, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze. If you have not been a victim of identity theft, you will need to include payment to the credit reporting agency to place, lift, or remove a security freeze by check, money order, or credit card.

To place a security freeze on your credit report, you must send a written request to each of the three major reporting agencies by regular, certified, or overnight mail at the addresses below:

Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com
Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com

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 the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Vera Bradley

VERA BRADLEY NOTIFIES CUSTOMERS OF PAYMENT CARD INCIDENT

FORT WAYNE, Ind., October 12, 2016 – Vera Bradley, Inc. (Nasdaq: VRA) ("Vera Bradley" or the "Company") today announced that it has taken action to investigate and address an incident affecting payment card data used at its retail stores.

Payment cards used at Vera Bradley store locations between July 25, 2016 and September 23, 2016 may have been affected. Not all cards used in stores during this time frame were affected. Cards used on verabradley.com were not affected. Information on steps customers may take to protect their information can be found at www.verabradley.com/protectingourcustomers.

On September 15, 2016, Vera Bradley was provided information from law enforcement regarding a potential data security issue related to our retail store network. Upon learning this information, Vera Bradley immediately launched an investigation with the assistance of a leading computer security firm to aggressively gather facts and determine the scope of the issue and promptly notified the payment card networks. Findings from the investigation show unauthorized access to Vera Bradley's payment processing system and the installation of a program that looked for payment card data. The program was specifically designed to find track data in the magnetic stripe of a payment card that may contain the card number, cardholder name, expiration date, and internal verification code as the data was being routed through the affected payment systems. There is no indication that other customer information was at risk.

Vera Bradley has stopped this incident and continues to work with the computer security firm to further strengthen the security of its systems to help prevent this from happening in the future. Vera Bradley continues to support law enforcement's investigation and is also working with the payment card networks so that the banks that issue payment cards can be made aware and initiate heightened monitoring on the affected cards.

Potentially affected customers are advised to remain vigilant to the possibility of fraud by regularly reviewing their payment card statements for any unauthorized activity. Customers should immediately report any unauthorized charges to their card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of the payment card.

Vera Bradley values the relationship it has with its customers and understands the importance of protecting personal information and therefore sincerely regrets any inconvenience this may have caused its customers. If customers have any questions, they may call 844-723-9340 from 9:00 a.m. to 9:00 p.m. EDT, Monday through Friday.