NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
Tabor Center
1200 17th Street, Suite 1000
Denver, Colorado 80202-5835
United States

Direct line +1 303 801 2758
kris.kleiner@nortonrosefulbright.com

Tel +1 303 801 2700
Fax +1 303 801 2777
nortonrosefulbright.com

May 12, 2017

Via E-Mail
(SecurityBreach@atg.wa.gov)

Office of the Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

Re: Legal Notice of Information Security Incident

Dear Sirs or Madams:

I write on behalf of my client, Brooks Brothers, to inform you of a potential security incident that may have affected the payment card information of some Washington residents. Unfortunately, because this incident impacted point-of-sale transactions, Brooks Brothers does not have the means to identify affected individuals or their state of residence. As a result, Brooks Brothers is notifying affected individuals via notice on its website and through media and is outlining some steps that potentially affected individuals may take to help protect themselves. Brooks Brothers is also notifying your office, out of an abundance of caution, in the event that any Washington residents were impacted.

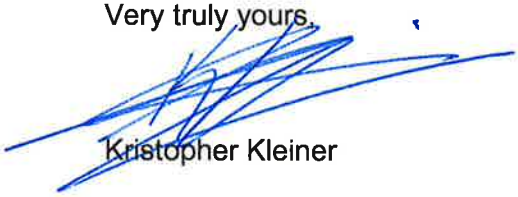
Brooks Brothers recently learned that an unauthorized individual was able to gain access to its network and install malicious software on its payment processing systems at certain locations designed to capture payment card information for transactions on point-of-sale terminals. The affected locations in Washington include Brooks Brothers retail and outlet stores in Auburn, Seattle and Tulalip. Based on the information currently available from Brooks Brothers' investigation, although not all transactions were affected, this incident may have impacted certain individuals who made payment card purchases at affected locations between April 4, 2016 and March 1, 2017.

Brooks Brothers takes the privacy of personal information very seriously, and deeply regrets that this incident occurred. Brooks Brothers took steps to address and contain this incident promptly after it was discovered, including engaging outside data forensic experts to assist in investigating and remediating the situation. Brooks Brothers has also contacted law enforcement and will continue to cooperate in their investigation of this incident.

Affected individuals are being notified via media notice and a notification on Brooks Brothers' website. A form copy of the website notice being provided to affected Washington residents is included for your reference.

If you have any questions or need further information regarding this incident, please contact me at (303) 801-2758 or kris.kleiner@nortonrosefulbright.com.

Very truly yours,



Kristopher Kleiner

KCK
Enclosure

Notice of Data Breach

Brooks Brothers recently became aware of a security incident that could affect the payment card information of some customers who made purchases at certain Brooks Brothers and Brooks Brothers Outlet retail locations in the U.S. and Puerto Rico only between April 4, 2016 and March 1, 2017. It is important to note that no sensitive personal information, such as social security number or personally identifying information, was affected in this incident. As a precaution, we are providing this notice to make potentially affected customers aware of the incident and provide information on steps they can take to help protect themselves. We take the security of our customers' information very seriously and value the trust you place in us to protect your information. We deeply regret any inconvenience or concern this may cause you.

What Happened

Brooks Brothers was recently alerted to a potential security incident. Based upon an extensive forensic investigation, it appears that an unauthorized individual was able to gain access to and install malicious software designed to capture payment card information on some of our payment processing systems at our retail and outlet locations. To find out if your Brooks Brothers or Brooks Brothers Outlet location was impacted, please visit www.brooksbrothers.com/incident-locations for a list of affected locations. Please note that this incident did not affect any purchases made on the BrooksBrothers.com website.

What Information Was Involved

Based on our investigation to date, we believe the malicious software could have affected payment card data – including name, payment card account number, card expiration date, and card verification code – of some customers who used a payment card at affected Brooks Brothers or Brooks Brothers Outlet locations. The incident did not affect Social Security numbers, customer addresses, or any other sensitive personal information. Although not all transactions were affected, the forensic investigation has indicated that this incident may have impacted certain individuals who made payment card purchases between April 4, 2016 and March 1, 2017.

What We Are Doing

We take the security of our customers' information very seriously and, once we learned of this incident, we took immediate action including initiating an internal review, engaging independent forensic experts to assist us in the investigation and remediation of our systems and alerting law enforcement. While we are continuing to review and enhance our security measures moving forward to help prevent a future incident, we can confirm that this issue has been resolved and is no longer impacting transactions.

What You Can Do

In order to help protect themselves, we recommend that customers review credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. We urge customers to remain vigilant and continue to monitor statements for unusual activity going forward. If they see anything they do not understand or that looks suspicious, or if they suspect that any fraudulent transactions have taken place, customers should immediately notify the issuer of the credit or debit card. In instances of payment card fraud, it is important to note that cardholders are typically not responsible for any fraudulent activity that is reported in a timely fashion.

Although this incident did not include Social Security numbers, addresses, or other sensitive personal information, as a general practice, we recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. As an additional precaution, we are providing information and resources to help customers protect their identities. This includes an "Information About Identity Theft" reference guide, which describes additional steps customers may take to help protect themselves, including recommendations from the Federal Trade Commission regarding identity theft protection.

For More Information

For more information about this incident, or if you have additional questions or concerns about this incident, you may contact us directly at 888-735-5927 between 9 a.m. and 9 p.m. Eastern time. Again, we sincerely regret any concern this incident may cause.

Sincerely,

Brooks Brothers

Information about Identity Theft Protection

Review Accounts and Credit Reports: You can regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You can 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 at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For residents of Maryland: You can also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For residents of North Carolina: You can also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Rhode Island You can also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, www.riag.ri.gov.

Fraud Alerts: There are also two types of fraud alerts that 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 at the addresses or toll-free numbers listed at the bottom of this page.

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.

Additional Information for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports. The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company. (By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.) You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): 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; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

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

National Credit Reporting Agencies Contact Information

Equifax (www.equifax.com)
General Contact:
P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts:
P.O. Box 740256, Atlanta, GA 30374
Credit Freezes:
P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)
General Contact:
P.O. Box 2002
Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
General Contact:
P.O. Box 105281
Atlanta, GA 30348
800-888-4213

Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
888-909-8872