

14739



<<Date>>

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip Code>>

Subject: Data Security Incident

Dear <<First Name>> <<Last Name>>:

I am writing to inform you of a data security incident that may have involved your personal information. At Blackstone Investment Group ("Blackstone"), we take the privacy and security of your information very seriously and regret any concern that this incident may cause you. This letter contains information about steps you can take to protect your information and resources we are making available to help you.

What Happened? On November 15, 2018, we discovered unusual activity relating to the webserver for the Blackstone owned website www.haikubags.com. As soon as we discovered the activity, we took immediate steps to secure the webserver and hired an independent computer forensics expert to assist with an investigation of the activity. The investigation revealed that an unauthorized individual obtained access to the webserver and may have accessed personal information belonging to some Blackstone customers. Though we are unaware of the misuse of any information involved in this incident, we are notifying you out of an abundance of caution.

What Information Was Involved? The information potentially impacted by this incident includes your name, username and password for the "Haikubags.com" website, and payment card information, including card number, expiration date, and security code.

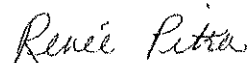
What we are doing? We are providing you with Cyber Monitoring services at no charge to you for twelve months. The cyber monitoring will review the dark web and alert you if your personally identifiable information is found online. In addition, we are providing you with fraud assistance to help with any questions that you might have on how to best prevent fraud from occurring as well as identity fraud resolution services in the event that you become a victim of fraud. These services will be provided by CyberScout, a company that specializes in identity theft education and resolution.

To enroll in Cyber Monitoring services at no charge, please log on to <https://www.myidmanager.com> and follow the instructions provided. When prompted, please provide the following unique code to receive services: <<Code Here>>. The deadline to enroll for these services is May 10, 2019.

What you can do? We recommend you review the enclosed information about steps you can take to protect your personal information. We also recommend you review your current and past financial account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the account immediately.

For More Information: We sincerely regret any inconvenience or concern that this matter may cause you and remain dedicated to protecting all information in our systems. Please do not hesitate to call 855-652-3700, Monday through Friday, 8:00 a.m. to 5:00 p.m. Central Time if you have questions about this event.

Sincerely,

A handwritten signature in cursive script that reads "Renee Pitra".

Renee Pitra
CEO
Blackstone Investment Group, Inc.

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your 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 incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 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 also contact one of the following three national credit reporting agencies:

Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 1000 Chester, PA 19016 1-877-322-8228 www.transunion.com	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 www.annualcreditreport.com
--	---	---	---

Fraud Alert: 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 the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission 600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov, and www.ftc.gov/idtheft 1-877-438-4338	Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	North Carolina Attorney General 9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	Rhode Island Attorney General 150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 401-274-4400
---	--	--	--

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.