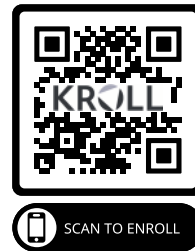




<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>



<<Date>> (Format: Month Day, Year)

NOTICE OF DATA BREACH

Dear <<First_name>>,

We are writing to notify you that Blackstone Inc. (“Blackstone”) recently experienced a cybersecurity incident and that some of your personal information was affected. Please read this notice carefully, as it provides up-to-date information on what happened and what we have done in response.

What Happened?

On July 23, 2026, an unauthorized party briefly gained access to a small number of Blackstone employee user accounts and was able to use that access to obtain copies of files from certain of our cloud-based file repositories. Upon learning of the unauthorized access, we promptly took steps to stop the access and conduct an investigation with the assistance of outside data security experts. We also reported the matter to law enforcement.

What Information Was Involved?

Our investigation has determined that some of your personal information was affected by this incident, including your <<b2b_text_1 (Data Elements)>>.

Blackstone does not have any indication that the unauthorized third party was targeting your personal information specifically or that there has been any actual misuse or dissemination of such information.

What We Are Doing

Blackstone takes this incident and our responsibility to protect personal information in our possession extremely seriously, and we have taken a range of steps to enhance our existing security controls.

As a precaution, we have engaged Kroll to provide 2 years of identity monitoring services at no cost to you. These services include credit monitoring, fraud consultation, and identity theft restoration services.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

If you have any questions about this service or need assistance with enrollment, please see the “For More Information” section below.

What You Can Do

We strongly encourage you to take advantage of the identity monitoring services we are providing to you free of charge. Remain vigilant and carefully review your online and financial accounts for any suspicious activity.

If you detect any suspicious activity on an account, you should change the password and security questions associated with the account, and promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incident of identity theft to the proper law enforcement authority.

If you would like to take additional steps to protect your personal information, we have attached helpful resources to this letter on how to do so, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file where relevant.

For More Information

Blackstone has established a dedicated call center to answer questions. If you have any questions regarding this incident or the services available to you, please call (844) 301-0220 between 8:00 am to 5:30 pm Central Time, Monday through Friday, excluding major U.S. holidays.

Once again, we sincerely regret that this incident occurred. We have taken robust steps to address it.

Sincerely,

Laura Weiss

Chief Data Counsel and Data Policy and Strategy Officer

Blackstone Inc.

Additional Resources

- You can learn more about how to protect yourself against identity theft by visiting www.usa.gov/identity-theft, or by contacting the Federal Trade Commission (FTC) or your state's Attorney General to obtain information, including about how to avoid identity theft, place a fraud alert, and place a security freeze on your credit report. **Federal Trade Commission**, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft
- **Order Your Free Credit Report:** We encourage you to periodically obtain credit reports from the below credit agencies and have fraudulent transactions deleted. To obtain an annual free copy of your credit reports, visit annualcreditreport.com, call toll-free at 1-877-322-8228, or contact the major credit reporting agencies. Their contact information is as follows:

Equifax:

equifax.com
equifax.com/freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-525-6285

Experian:

experian.com
experian.com/freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion:

transunion.com
transunion.com/freeze
P.O. Box 2000
Chester, PA 19016
1-888-909-8872

- **Fraud Alert:** You may place a fraud alert in your file by contacting one of the three nationwide credit reporting agencies listed above. A fraud alert puts creditors on notice that you might be a victim of fraud. Creditors will then follow certain procedures designed to protect you, including contacting you before they open new accounts or change your existing accounts. Placing a fraud alert can protect you but also may delay you when you seek to obtain credit.
- **Security Freeze:** You have the ability to place a security freeze on your credit report at no charge. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent but may delay your ability to obtain credit. To place a security freeze, you must contact each of the three credit bureaus listed above and may be required to provide your full name; SSN; date of birth; the addresses where you have lived over the past five years; proof of current address, such as a utility bill or telephone bill; a copy of a government issued identification card; and if you are the victim of identity theft, the police report, investigative report, or complaint to a law enforcement agency.
- **Fraud or Identity Theft:** If you suspect theft, you should file a report to law enforcement, the FTC at www.identitytheft.gov, or the Attorney General in your state. If you are the victim of fraud or identity theft, you have the right to (1) notify the police and Attorney General of your state; and (2) file a police report relating to the incident and obtain a copy of the report.
- **Federal Fair Credit Reporting Act Rights:** The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies (CRAs) use your information. The FTC has summarized consumers' FCRA rights as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to a credit score; you have the right to dispute incomplete or inaccurate information; CRAs must correct or delete inaccurate, incomplete, or unverifiable information; CRAs may not report outdated negative information; access to your file is limited; employers need your consent to receive your reports; you may limit "prescreened" credit and insurance offers based on your credit report; you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights. For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580.
- **State-Specific Notices.** Residents of the following states should review the following information:
 - **For District of Columbia residents:** You may contact the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://www.oag.dc.gov/>, 1-202-727-3400.
 - **For Maryland residents:** You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, <http://www.marylandattorneygeneral.gov/>, 1-888-743-0023.
 - **For New York residents:** You may consider placing a Security Freeze on your credit report. For more information on a Security Freeze or on how to avoid identity theft, contact the New York Department of State Division of Consumer Protection (<http://www.dos.ny.gov/consumerprotection/>; (800) 697-1220) or the New York State Office of the Attorney General (<http://www.ag.ny.gov/home.html>; (800) 771-7755).

- **For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, <http://www.ncdoj.gov/>, 1-877-566-7226 to contact other nationwide consumer reporting agencies and to make freeze requests and obtain information on combating identity theft.
- **For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. For more information about placing a security freeze, you can visit the Oregon Department of Justice Consumer Protection website at <https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/>.
- **For Vermont residents:** Helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report is available on the Vermont Attorney General's website at <http://www.ago.vermont.gov>. If you do not have Internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802- 656-3183 (800-649-2424 toll free in Vermont only).
- **For Rhode Island residents:** For more information on how to prevent identity theft, you may contact the Rhode Island Attorney General at 150 South Main Street, Providence, RI 02903, (401) 274-4400, and <https://riag.ri.gov/>. You have the right to obtain a police report about this incident. You may be required to pay fees to a consumer reporting agency when placing a credit freeze on your credit file. There were 3 Rhode Island residents impacted by this incident.