

NOTICE OF DATA SECURITY INCIDENT

Black, Gould & Associates, Inc. (“BGA”) is making individuals aware of an incident that may affect the privacy of certain information. Although BGA is unaware of any actual or attempted misuse of such information, we are providing notice of the event so potentially affected individuals may take steps to better protect their information from misuse, should they feel it appropriate to do so.

What Happened? On or about September 9, 2022, BGA discovered unusual activity within its environment. BGA promptly took steps to secure its systems, and with the assistance of third-party forensic specialists, conducted an investigation to confirm the nature and scope of the incident. Through the investigation, BGA identified unauthorized access within its environment between August 31, 2022 and September 10, 2022. BGA undertook a thorough review of the potentially affected files to determine whether any potentially sensitive information was present within them.

On September 21, 2022, BGA confirmed the population of individuals whose information was included in the affected files. On October 13, 2022, BGA notified relevant brokers that certain information may have been impacted. After confirming with its brokers, BGA then proceeded promptly with direct notifications to individuals for whom address information was available.

What Information Was Involved? Although the data in the impacted systems may vary by individual, the data may have contained the following types of information at the time of the incident: names, date of birth, and Social Security numbers. BGA is sending written notification to all potentially impacted individuals for whom we could obtain address information.

What is BGA Doing? The confidentiality, privacy, and security of information within BGA’s care are among BGA’s highest priorities. BGA responded immediately to this incident, promptly notified law enforcement authorities, and has been working diligently to provide individuals with an accurate and complete notice of the incident as soon as possible. BGA also took steps to secure potentially affected systems and conduct a diligent investigation aided by third-party cybersecurity specialists. Further, BGA implemented additional technical security measures designed to mitigate and minimize the recurrence of a similar future incident. In an abundance of caution, BGA is also notifying potentially affected individuals and providing information on steps that may be taken to best protect personal information.

What You Can Do. BGA encourages individuals to remain vigilant against incidents of identity theft and fraud by reviewing their account statements and monitoring their free credit reports for suspicious activity and to detect errors. Individuals may also review and consider the information and resources outlined in the below “*Steps Individuals Can Take to Protect Information.*”

For More Information. If individuals have additional questions, please call our dedicated assistance line at (833) 814-1737, Monday through Friday from 9 am - 9 pm Eastern Time, excluding U.S. holidays, or go to <https://response.idx.us/bga>. You may also write to BGA at: Compliance Department, Black, Gould & Associates, Inc., 3800 N. Central Avenue, 9th Floor, Phoenix, Arizona 85012.

STEPS YOU CAN TAKE TO PROTECT INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

Full name (including middle initial, as well as Jr., Sr., II, III, etc.);

1. Social Security number;
2. Date of birth;
3. Addresses for the prior two to five years;
4. Proof of current address, such as a current utility bill or telephone bill;
5. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
6. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016

Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094
--	---	--

Additional Information

If any individuals had a username and password involved in this incident, we recommend those individuals change the password and any security question or answer for those accounts immediately. If individuals reuse usernames and passwords for other online accounts, it is recommended those individuals change the password and any security question or answer for those online accounts, as well. Further, as a general precaution, individuals should never use the same password for more than one online account. When creating passwords, they should be complex and not contain personal information.

Individuals may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Individuals can obtain further information on how to file such a complaint by way of the contact information listed above. Individuals have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, individuals will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the state Attorney General. This notice has not been delayed by law enforcement.

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.