

P



October 02, 2025

Dear ,

We are writing to inform you of a data security incident that may have impacted some of your personal information. We take the security of your information and any concern this incident may cause very seriously. This letter contains information about what happened, actions we have taken to prevent a reoccurrence, and steps you can take to protect your information.

What Happened?

Recently, we were the target of a cyber-attack. We immediately notified law enforcement, moved quickly to contain the incident, and conducted a thorough investigation with the assistance of computer forensic experts. We believe it likely that the attacker only wanted money and not the information on our computers but, in an abundance of caution, we are letting you know that some of your personal information may have been accessed by the attackers.

What Information was Involved?

On September 10, 2025, we discovered that some documents accessed may have contained information including your .

What We Are Doing.

The security of all information in our systems is taken very seriously, and we want to assure you that we've already taken steps to prevent a reoccurrence by enhancing security measures and security monitoring and increasing company awareness of data security protection.

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How You Enroll In the Free Services

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services:

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

000010102G0400

P

What You Can Do

Although we have no reports of misuse of your or anyone's information, we encourage you to follow the instructions in this letter and enroll in the identity protection services we are providing at no cost to you. We also recommend that you review the "Additional Important Information" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission (FTC) regarding identity theft protection and details on how to place a fraud alert or security freeze on your credit file. As an added precaution, you may want to closely monitor your personal accounts for any suspicious activity.

For More Information

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays. Please call the help line 1- 833-833-7219 and supply the fraud specialist with your unique code listed above.

We appreciate your patience and understanding, and we sincerely apologize for any inconvenience or concern the incident may cause you.

Sincerely,
Glenwood Management

Additional Important Information

Monitoring: You should always remain vigilant for incidents of fraud and identity theft, especially during the next 12-24 months, by reviewing financial account statements and monitoring your credit reports for suspicious or unusual activity and immediately report any suspicious activity or incidents of identity theft. You have the right to obtain or file a police report. You can contact the Federal Trade Commission (FTC) for more information on preventing identity theft. We encourage you to report any incidents of identity theft to the FTC.

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



Credit Reports: You may obtain a copy of your credit report, for free, whether or not you suspect any unauthorized activity on your account, from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You have the right to place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center.html) or TransUnion (www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. To place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be needed to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-reports-services/credit-freeze/
1-866-478-0027

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013-9544
<http://www.experian.com/freeze/center.html>
1-888-397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
1-800-916-8800

For residents of Iowa and Oregon: You are advised to report any suspected identity theft to law enforcement or to the state Attorney General and Federal Trade Commission.

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission.

Massachusetts and Rhode Island residents: You have the right to obtain or file a police report.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island:

You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the FTC about fraud alerts, security freezes, and steps you can take to prevent identity theft. There were 13 Rhode Island residents notified in this incident.

District of Columbia	Maryland	Office of	New York	North Carolina	Rhode Island
Attorney General	Attorney General		Attorney General	Attorney General	Attorney General
400 6 th Street NW	200 St. Paul Pl		120 Broadway, 3rd Fl	9001 Mail Service Ctr	150 South Main St
Washington, DC	Baltimore, MD 21202		New York, NY 10271	Raleigh, NC 27699	Providence RI 02903
20001	1-888-743-0023		1-800-771-7755	1-877-566-7226	1-401-274-4400
1-202-442-9828	https://www.marylandattorneygeneral.gov/		www.ag.ny.gov	https://ncdoj.gov/	www.riag.ri.gov
www.oag.dc.gov					