

Tarter Krinsky & Drogin LLP
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024



111 *****AUTO**All For SCF 303



September 4, 2026

NOTICE OF SECURITY INCIDENT

Dear [REDACTED]:

Tarter Krinsky & Drogin LLP (“TKD”) writes to inform you of an event that may affect the security of some of your information. TKD is a law firm assisting its clients with legal services. Our clients include one of your healthcare providers, and through that representation, we were in possession of certain protected health information. Although we are unaware of any identity theft or fraud occurring as a result of this event, we are providing you with information about the event, our response, and resources available to help you protect your information, should you feel it appropriate to do so.

What Happened? On September 10, 2025, TKD became aware of suspicious activity within its environment. We then immediately launched an investigation into the nature and scope of the activity with the assistance of third-party forensic specialists. The investigation determined that there was unauthorized access to certain TKD servers at various times between July 9, 2025 and September 9, 2025, and that certain information stored within those servers was viewed or obtained by the unauthorized actor during that time period. Upon learning of this information, TKD undertook a comprehensive review of the affected files, with the assistance of third-party subject matter specialists, to attempt to identify what information was contained, therein and to whom that information related. That review has recently been completed, and TKD is notifying you upon determining that certain information related to you was contained within the potentially affected files.

What Information Was Involved? Our investigation and review determined that your name and the following types of information related to you were found in the potentially affected files: [REDACTED]. Please note that TKD is not aware of any attempted or actual misuse of your information, or that your information was used to commit identity theft or fraud.

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities. We promptly notified federal law enforcement upon becoming aware of the referenced suspicious activity. We are reviewing existing security policies and have implemented additional cybersecurity measures to further protect against similar events moving forward. We are also notifying potentially impacted individuals, including you, so you may take steps to best protect your information, should you feel it is appropriate to do so.

[REDACTED]

As an added precaution, we are also offering you immediate 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 twelve 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. You can find information on how to enroll in these services in the enclosed *Steps You Can Take to Help Protect Personal Information*. We encourage you to enroll in these services as we are not able to do so on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may also enroll in the complimentary credit monitoring services we are offering. Please also review the information contained in the enclosed *Steps You Can Take to Help Protect Personal Information*.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please contact 1-877-520-3879, Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern time, excluding major U.S. holidays. You may also write to us at 1350 Broadway, New York, New York 10018. We take this event very seriously and sincerely regret any inconvenience or concern this event may cause you.

Sincerely,

Tarter Krinsky & Drogin LLP



STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Identity Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to the following link:
<https://bfs.cyberscout.com/activate>

Please then follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]

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.

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 1-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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

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

Should consumers wish to place a credit freeze or fraud alert, 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	1-833-799-5355



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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your 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, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers 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, consumers 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 relevant 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, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 90 Rhode Island residents that may be impacted by this event.

