BakerHostetler

Baker&Hostetler LLP
Washington Square, Suite 1100
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5403
T 202.861.1500
F 202.861.1783
www.bakerlaw.com

Jon R. Knight
direct dial: 202.861.1664
jknight@bakerlaw.com

January 31, 2025

VIA EMAIL (IDTHEFT@OAG.STATE.MD.US)

Anthony G. Brown
Attorney General
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Incident Notification

Dear Attorney General Brown:

I am writing on behalf of my client, SciTech Services, Inc. ("SciTech"), to notify you of a security incident involving 182 Maryland residents.

On October 30, 2024, SciTech detected unusual activity within its network. Upon detecting the unusual activity, response protocols were implemented, measures were taken to contain the activity, and an investigation was launched. Additionally, SciTech engaged a cybersecurity firm that has assisted other business with similar situations to assist with the investigation. The investigation identified unauthorized access to and encryption of certain systems within SciTech's network on October 30, 2024. During this time, an unauthorized entity acquired files stored within SciTech's network.

The files involved were carefully reviewed and it was determined that the files contained the name, address, and Social Security number of 182 Maryland residents. The files also contained one or more of the following for the 182 Maryland residents: date of birth, driver's license number, or passport number. For some residents, financial account information or the results of a physical examination were also included.

On January 31, 2025, SciTech will mail notification letters via United States Postal Service First-Class mail to the Maryland residents whose information may have been involved in accordance with Md. Code Ann., Com. Law § 14-3504. A sample notification letter is enclosed. SciTech is offering a complimentary 12-month membership to credit monitoring and identity protection services for the Maryland residents whose Social Security numbers were involved.

To help prevent this type of incident from happening again, SciTech continues to monitor the network and continues to take steps to enhance already existing security measures.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Jon R. Knight,
Counsel

Enclosures

SciTech Inc.
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS18

0_0000256

0000256

SciTech Services Inc.

[redacted]

January 31, 2025

Dear [redacted]:

SciTech Services, Inc. ("SciTech") recognizes the importance of protecting information. We are writing to notify you of a security incident involving your information. This letter explains the incident, measures we have taken, and additional steps you may consider taking in response.

What Happened? On October 30, 2024, SciTech became aware of a potential data security incident impacting SciTech's systems. We immediately launched an investigation and sought assistance from a cybersecurity firm experienced in managing similar scenarios. The investigation identified unauthorized access to and encryption of certain systems within our network on October 30, 2024. During this time, an unauthorized entity acquired files stored within our network.

What Information Was Involved? We reviewed the available evidence of the files involved and determined the files likely contained information related to your employment verification and/or taxes. The personal information included your name, Social Security number and one or more of the following: date of birth, address, driver's license number, or passport number. Your financial account information was also involved.

What We Are Doing. We wanted to notify you of this incident and to assure you that we take it seriously. To help prevent something like this from happening again, we have taken and are taking steps to enhance our existing security measures. We notified law enforcement about the incident and will continue to support law enforcement's investigation.

What Can You Do? Additionally, we have arranged for you to receive one year of free access to credit monitoring and identity protection services through Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. This product is designed to detect potential misuse of your information and offers identity protection solutions aimed at promptly identifying and resolving any instances of identity theft. Activating this product will not impact your credit score negatively. For more information on identity theft prevention and this service, including instructions on how to activate your access, as well as some additional precautionary measures you can take, please review the pages that follow this letter.

For More Information. The privacy and security of data entrusted to SciTech is of the utmost importance to us. We sincerely regret this occurrence and apologize for any concern that it may cause you. Should you have any questions regarding the incident, please do not hesitate to contact us at 1-800-405-6108. The call center is available Monday to Friday, between 8:00 am to 8:00 p.m. Eastern Time, excluding major U.S. holidays.

Sincerely,

SciTech Services, Inc.

Instructions for Enrolling In Credit Monitoring

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 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.

How do I enroll for 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: [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.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-833-799-5355

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
TransUnion Security Freeze, PO Box 160, Woodlyn, PA 19094, www.transunion.com
Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

SciTech Services, Inc. is located at 2129 Pulaski Highway, Suite 100, Havre de Grace, MD 21078 or by phone at 443-303-3623.

Additional information for residents of the following states:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

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 ask for a credit score.
You have the right to dispute incomplete or inaccurate information.
Consumer reporting agencies 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 reports to be provided to employers.
You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
You may seek damages from violators.
Identity theft victims and active duty military personnel have additional rights.