

Houston-Galveston Area Council
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111



F-4409

[REDACTED]
[REDACTED]
[REDACTED]

April 26, 2022

Dear [REDACTED]:

Notice of Data Breach

At Houston-Galveston Area Council, we take the privacy and security of personal information very seriously. We are writing to let you know about a data security incident we recently addressed that involved some of your personal information. This notice explains the incident, measures we have taken in response, and some steps you may consider taking to help protect your information.

What Happened?

On December 29, 2021, H-GAC learned of suspicious activity within our network. We immediately launched an investigation with the assistance of cybersecurity and forensic specialists and took steps to ensure the security of our network. Our investigation determined that an unauthorized individual had accessed H-GAC's network, deployed ransomware, and downloaded files from our network. We conducted a review of the involved files and determined, in March of 2022, that some of those files include your personal information. While we have no knowledge of any misuse of any personal information as a result of this incident, we wanted you to be aware and to know that we take it seriously.

What Information Was Involved?

The files that were downloaded contain information relating to you which may include your name, address, and information about your medical history, health insurance claims, health insurance policy number, and/or other health-related information.

What We Are Doing.

The privacy and security of personal information is one of our highest priorities and H-GAC has security measures in place to protect information in our care. Upon discovering this incident, we immediately took steps to investigate this incident and further secure our network.

What You Can Do.

While there is no evidence that any of your information was misused as a result of this incident, we nonetheless encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. For additional information on steps you can take to protect your identity, please review the information included with this letter.

For More Information.

We recognize that you may have questions not addressed in this letter. For more information, or if you have any questions or need additional information, please call (888) 603-2588 between 8:00 AM and 5:00 PM Central time, Monday through Friday.

We sincerely regret any inconvenience this incident may cause you. Protecting information entrusted to H-GAC is very important to us, and we remain committed to safeguarding the information in our care.

Sincerely,

A handwritten signature in black ink, appearing to read 'CW', written in a cursive style.

Chuck Wemple
Executive Director

ADDITIONAL STEPS YOU CAN TAKE

Free Credit Report. Regardless of whether you choose to take advantage of the complimentary identity monitoring, 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. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. 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. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 105788 Atlanta, Georgia 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 2390 Allen, Texas 75013 www.experian.com	Phone: 1-800-888-4213 P.O. Box 1000 Chester, PA 19016 www.transunion.com

For Colorado and Maryland residents:

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

Don't confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. You may obtain information from the credit reporting agencies and the FTC about security freezes.

Upon receiving a request for a security freeze, each credit bureau will provide you with a unique identification number or password. Keep the number or password secure, as you will need it if you choose to lift the freeze. If you request a freeze be lifted (either temporarily or entirely), a credit bureau must lift the freeze within one hour if it is requested online or via phone. If requested by mail, a credit bureau must lift the freeze no later than three business days after receipt.

Fraud Alerts. You may ask that a fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. 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. You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

Federal Trade Commission and State Attorneys General Offices. 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 home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

Reporting of identity theft and obtaining a police report.

You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

If you know or suspect you are a victim of tax-related identity theft, the IRS recommends these steps:

Respond immediately to any IRS notice; call the number provided or, if instructed, go to IDVerify.irs.gov.

Complete IRS Form 14039, Identity Theft Affidavit, if your e-filed return rejects because of a duplicate filing under your SSN or you are instructed to do so. Use a fillable form at IRS.gov, print, then attach the form to your return and mail according to instructions.

Continue to pay your taxes and file your tax return, even if you must do so by paper.

If you previously contacted the IRS and did not have a resolution, contact the IRS for specialized assistance at 1-800-908-4490.