Elmhurst Development LLC

C/O
P.O. Box 3826
Suwanee, GA 30024

September 5, 2024

Notice of Data Incident

Dear <<first name>><<last name>>:

Elmhurst Development LLC ("Elmhurst," "we," or "us") is writing to inform you about a recent cybersecurity incident that may have impacted some of your personal information. The security of your personal information is very important to us, and we take the trust you place in us very seriously. We wanted to advise you about the incident and to offer you some resources you may find helpful.

What Happened? Elmhurst recently detected unauthorized activity in our IT systems. Upon discovering this activity, we immediately took protective actions to stop any unauthorized access, notified U.S. federal law enforcement, and launched an investigation with the assistance of leading cybersecurity specialists. The investigation so far indicates that some of your personal information may have been accessed by an unauthorized party as early as mid May 2024. Due to an encryption event, we were unable to determine the scope of unauthorized access until late July 2024. At this time, we have no reason to believe your information has been misused; however, we are providing you notice out of an abundance of caution.

What Personal Information May Be Involved? The affected personal information may have included your <<data elements>>.

What We Are Doing. We are taking this incident very seriously. Upon detecting unauthorized activity in our IT system, we took immediate protective actions to contain the activity and retained industry-leading cybersecurity specialists. It is our priority to continue to evaluate and deploy the level of robust security protocols, continuous monitoring, and staff training needed to prevent and defend against sophisticated cybersecurity threats.

What You Can Do. Because our investigation indicated that some of your personal information may have been affected, we are offering you a 24-month membership in the Haystack credit monitoring and identity restoration services, by HaystackID, at no cost to you. These services include 3-bureau credit monitoring services with email alerts and a once annual credit report and score through TransUnion. This program, which is detailed in the section below, will help you to quickly detect any compromise or possible misuse of your personal information.

To enroll in the credit monitoring services at no charge, please use the following verification code, <<code>>. We encourage you to contact HaystackID with any questions and to enroll in the free identity protection services by calling 855-508-3823 or going to www.haystackid-notifications.com. Please note the deadline to enroll is December 2, 2024.

Again, we take very seriously the security and privacy of your information, and we want to make sure you have the information you need so that you can take steps to help protect your personal data. We recommend you remain vigilant to the possibility of fraud and identity theft by reviewing and monitoring your account statements and free credit reports for any unauthorized activity. If you find any unauthorized or suspicious activity, you should immediately contact your credit card company, financial institution, and/or law enforcement.

For More Information. We sincerely regret any inconvenience this incident may cause you. If you have any questions regarding this incident or the services available to you, please call the HaystackID call center at 855-508-3823 (excluding major U.S. Holidays):
Eastern Time: Monday to Friday 9:00 AM to 9:00 PM.

Sincerely,

Elmhurst Development LLC

IDENTITY THEFT PROTECTION PLAN BENEFITS DESCRIPTIONS

Three Bureau Credit Monitoring with Email Alerts as Applicable: Monitors and alerts an individual when certain types of new activity appear on the Equifax, Experian, and TransUnion credit files. This includes positive and negative reason codes and incorporates non-traditional data to expand the scorable population by 30-35M individuals. Considers at least 24 months of credit history (including utilities, rent and telco when available) for increased predictiveness.

Once Annual Bureau Credit Report and Score: Provided through TransUnion. Shows updates to your score as well as any other activity that would reflect on your credit report. Accessible through your HaystackID portal.

Identity Monitoring with Proactive Phone Alerts: Proprietary algorithms search and monitor thousands of databases and 300 billion records (99% of U.S. adult individuals) searching for suspicious activity that could indicate the beginning steps of identity theft. We do not require a individual to provide personal information such as a Social Security number or date of birth to protect and monitor for suspicious activity. The individual supplies name, address, and phone number (email address optional) to create a data profile, then compares that information with our databases to identify suspicious activity and make a personal alert phone call, if necessary.

Identity Risk Scores: A proactive scoring solution based on data, not demographics, to help individuals identify their level of identity theft risk. This is not a credit score or credit rating. A risk score is generated by applying proprietary analytics to 300 billion records (99% of U.S. adult individuals) and thousands of databases to create a risk score between 0 and 999. If relevant information is found that affects risk, the score changes.

Free Annual Credit Report Access and Reminder Service (All 3 Bureaus): Provides easy access to federally mandated free credit reports from Experian, Transunion, and Equifax, along with a reminder service to request reports every four months (if individual's email address is provided).

High Risk Monitoring - Account Activity Alerts: We monitor participating banks, online retailers, telecom providers, health insurers and more looking for suspicious activity that could indicate the beginning steps of identity theft to both the individual's current accounts and new accounts. These are alerts that typically take place outside of a credit report and expose individuals to financial risk. Once in the secure area, the individual has the option to enter a Social Security number to activate this benefit. HaystackID does not store SSNs or use them for any other purpose.

Dark Web Monitoring: Our intelligent dark web monitoring searches tens of millions of sources across the surface, deep and dark web for compromised information. We then send a real-time alert to individuals whose identities may have been compromised so they can take protective action immediately, such as changing passwords or closing down email accounts. Information we scan for includes driver's license number, passport, address, medical ID, credit and debit cards, bank accounts, phone numbers and email addresses.

$1,000,000 Identity Theft Event Insurance with $0 Deductible – Discovery Based: Provides up to $1,000,000 ($0 deductible) Identity Theft Event Expense Reimbursement Insurance on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

$1,000,000 Unauthorized Electronic Funds Transfer Insurance with $0 Deductible – Occurrence Based: Provides up to $1,000,000($0 deductible) Unauthorized Electronic Funds Transfer Reimbursement. This aids in the recovery of stolen funds resulting from fraudulent activity.

Fully Managed Identity Restoration – U.S. Based (No Signup Required): Should identity theft occur, HaystackID's restoration vendor does whatever it takes to restore the individual's name to pre-identity theft status. This benefit has an unlimited service guarantee and will spend whatever it takes in restoring the individual's identity and good name to a pre-theft status.

Social Security Statement Access and Reminder (Online Only): Provides easy access to online Social Security statements and a reminder tool for individuals to access statements every four months. If unknown income is shown, the individual may identify that as suspicious activity.

Lost Wallet/Purse: Uses multi-party calls to cancel/reissue credit cards and close bank accounts. We do not ask a individual to enter personal information such as credit/debit card numbers, driver's license number, and medical health numbers on our website. Instead, we have our Fraud Resolution Specialists provide personal telephone assistance.

Quarterly Online Newsletter: A quarterly e-newsletter educating individuals on identity theft protection.

Monthly Email If No Suspicious Activity Found (Email Required): An email notification sent every 30 days if no suspicious activity is detected.

RECOMMENDED STEPS FOR IDENTITY THEFT PROTECTION

Review Your Credit Reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia Residents: Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, https://oag.dc.gov, or by phone at (202) 442-9828.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division Office**,** 44 North Potomac Street, Suite 104, Hagerstown, MD 21740**,** Telephone: 1-888-743-0023, or at https://www.marylandattorneygeneral.gov/Pages/contactus.aspx

Massachusetts Residents: You are advised of your right to obtain a police report in connection with this incident.

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 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 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 a 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. You can 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.

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

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.