ENCON Heating & Air Conditioning
c/o Cyberscout
<Return Address>
<City>, <State> <Zip>

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<PostalCode+4>>

September 12, 2025

Re: Notice of Security <<Custom Field 1>>

Dear <<FirstName>> <<LastName>>:

I am writing to let you know that ENCON Heating & Air Conditioning ("ENCON" or the "Company") experienced a security incident that resulted in unauthorized access to some of our computer systems. The good news is that our information security defenses did prevent the attempted encryption of our network.

Our HR benefits and payroll systems, including Paylocity and Service Titan, were not affected and remain secure. However, you are receiving this notice because we found your personal information in some of the HR files stored locally on our computer network that were accessed and acquired.

What Happened? Computer systems within our network were accessed by an unauthorized third party who initially evaded detection by our information security defenses. Upon discovering the situation on February 24, 2025, we notified law enforcement and engaged cybersecurity experts to investigate. Through those efforts, we determined that a criminal threat actor had access to portions of our network between February 21 and February 24, 2025. Over the last few months, we conducted an in-depth review of our computer systems to identify which files were accessed and determine if any of those files contained personal information. We are notifying you now that we know what information was involved.

What Information Was Involved? We located records containing your individual name, along with <<Exposed Data Elements>>. We have not received any reports of any personal information being misused.

What We Are Doing. We are committed to protecting the personal information we maintain here at ENCON. Steps were taken to secure the deletion of any acquired files; we also retained a third party service to monitor online forums and marketplaces to verify the absence of any information relating to this event following the incident. We also have added some network requirements to fortify the security of our environment.

What You Can Do. We have no indication that any personal information has been misused as a result of this incident, nor do we expect this to occur. Nevertheless, we have enclosed instructions on how to enroll in a completely complimentary credit monitoring service for the next <<Service Length>>. If you are interested in this service, you can enroll online. Enrollment in this service is completely free, and doing so does not affect your credit score. We are also enclosing several informational resources to learn more about steps that can be taken to address any concerns you may have about identity theft or fraud.

For More Information. If you have any questions about this incident, or to activate the complimentary credit monitoring service, please reach out to our dedicated support team at [redacted] from 8:00 am to 8:00 pm EDT, Monday through Friday (excluding major U.S. holidays). For any other questions related to the incident, please contact [redacted]@goencon.com.

Sincerely,

[redacted] P.E., C.E.M.

IDENTITY PROTECTION REFERENCE GUIDE

1. Review your Credit Reports. We recommend that you monitor your credit reports for any activity you do not recognize. Under federal law, you are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To order your free annual credit report, visit www.annualcreditreport.com, call toll-free (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

If you see anything in your credit report that you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

2. Place Fraud Alerts. 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. Please note that placing a fraud alert may delay you when seeking to obtain credit. You can learn more about fraud alerts by contacting the credit bureaus or by visiting their websites:

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	1-800-888-4213
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

It is only necessary to contact <u>one</u> of these bureaus and use only <u>one</u> 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 should receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

3. Place Security Freezes. By placing a security freeze, someone who fraudulently acquires your personally identifying information will not be able to use that information to open new accounts or borrow money in your name. Federal and state laws prohibit charges for placing, temporarily lifting, or removing a security 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.

To place a security freeze, you must contact <u>each</u> of the three national credit reporting bureaus listed above and provide the following information: (1) your full name; (2) your social security number; (3) date of birth; (4) the addresses where you have lived over the past two years; (5) proof of current address, such as a utility bill or telephone bill; (6) a copy of a government issued identification card; and (7) if you are the victim of identity theft, include the police report, investigative report, or complaint to a law enforcement agency. If the request to place a security freeze is made by toll-free telephone or secure electronic means, the credit bureaus have one business day after receiving your request to place the security freeze on your credit report. If the request is made by mail, the credit bureaus have three business days to place the security freeze on your credit report after receiving your request. The credit bureaus must send confirmation to you within

five business days and provide you with information concerning the process by which you may remove or lift the security freeze.

4. Request an IP PIN from the IRS. Although the IRS is capable of identifying suspicious tax returns, taxpayers may choose to take proactive steps to prevent fraud, including obtaining an Identity Protection PIN (IP PIN) from the IRS. The IP PIN is a 6-digit number that, when active, will be required to file a tax return using the taxpayer's SSN or ITIN. To request an IP PIN, visit https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

In addition, taxpayers may opt in to ID.me, an identity verification service that requires a photo ID or live video session before logging in to submit a tax return online.

Finally, taxpayers may submit IRS Form 14039, Identity Theft Affidavit online if they received IRS correspondence indicating they might be a victim of tax-related identity theft or if their e-file tax return was rejected as a duplicate. After submitting the form, the IRS will refer the taxpayer's case to the Identity Theft Victim Assistance organization to investigate the case, remove fraudulent returns, and process the correct return and refund.

5. Monitor Your Account Statements. We encourage you to carefully monitor your financial account statements for fraudulent activity and report anything suspicious to the respective institution or provider.

6. You can also further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, your state Attorney General, or the Federal Trade Commission (FTC). The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (877-438-4338); and TTY: 866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

District of Columbia Residents: You can obtain additional information about identity theft prevention and protection from the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, (202) 727-3400, https://oag.dc.gov/.

Iowa Residents: You can report suspected identity theft to law enforcement, the FTC, or to the Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, 1-888-777-4590, https://www.iowaattorneygeneral.gov/.

Maryland Residents: You can obtain additional information about identity theft prevention and protection from the Maryland Attorney General, Identity Theft Unit at: 200 St. Paul Place, 25th Floor, Baltimore, MD 21202, 1-866-366-8343 or (410) 576-6491, https://www.marylandattorneygeneral.gov.

Massachusetts Residents: You have a right to file a police report and obtain a copy of your records. You can obtain additional information about identity theft prevention and protection from the Office of Consumer Affairs and Business Regulation, 501 Boylston Street, Suite 5100, Boston, MA 02116, (617) 973-8787, https://www.mass.gov/service-details/identity-theft.

New York Residents: You can obtain additional information about identity theft prevention and protection from the New York State Attorney General, The Capitol, State Street and Washington Avenue, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/.

North Carolina Residents: You can obtain additional information about preventing identity theft from the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free within North Carolina) or (919) 716-6000, https://ncdoj.gov/.

Oregon Residents: You can report suspected identity theft to law enforcement, the FTC, or the Oregon Office of the Attorney General at: Oregon Department of Justice, 1162 Court St NE, Salem, OR 97301, 1-800-850-0228, https://www.doj.state.or.us/.

Rhode Island Residents: You can obtain additional information about identity theft prevention and protection from the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, https://riag.ri.gov/. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services. There are approximately [#] Rhode Island residents that may be impacted by this event.

DETAILS REGARDING YOUR CYBERSCOUT MEMBERSHIP

We are offering you complimentary access to **Triple Bureau Credit Monitoring/Triple Bureau Credit Report/Triple Bureau Credit Score** services at no charge. These services provide you with alerts for <<Service Length>> 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.

To activate your membership and start monitoring your credit, please follow the steps below:

- Ensure that you **enroll within 90 days from the date of this letter** (Your code will not work after this date.)
- **Visit** the Cyberscout website to enroll: **https://bfs.cyberscout.com/activate**
- Provide your **unique code**: **<UniqueCode>**

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.**