

EXHIBIT 1

By providing this notice, Middleton does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of the Nebraska data event notification statute, or personal jurisdiction.

Nature of the Data Event

On September 6, 2024, Middleton became aware of suspicious activity within its computer network. Middleton immediately took steps to secure their systems and launched an investigation into the nature and scope of the activity with the assistance of third-party forensic specialists. The investigation determined that an unauthorized actor accessed Middleton's systems at various periods of time from September 1, 2024, to September 8, 2024, and certain information contained within those systems was viewed or copied by the unknown actor. Middleton therefore undertook a comprehensive and time-intensive review of the data at risk to determine what information was potentially affected, and to whom that information related. Those efforts recently completed, and Middleton provided notification to potentially impacted individuals.

The information that could have been subject to unauthorized access includes name, Social Security Number, and driver's license/state identification.

Notice to Nebraska Resident

On or about February 6, 2024, Middleton began providing written notice of this incident to approximately one (1) Nebraska resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon becoming aware of the event, Middleton moved quickly to investigate and respond, assess the security of Middleton systems, and identify potentially affected individuals. Middleton also notified federal law enforcement regarding the event. Middleton is also working to implement additional safeguards and training to its employees. Middleton is providing access to credit monitoring services for one (1) year, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Middleton is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Middleton is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Middleton is also providing written notice of this incident to relevant state regulators where required.

EXHIBIT A



P.O. Box 989728
West Sacramento, CA 95798-9728

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

February 6, 2025

<<NOTICE OF DATA BREACH>>

Dear <<Name 1>> <<Name 2>>:

Middleton Heat & Air, Inc. ("Middleton") writes to inform you of a recent event that may affect the confidentiality of information related to you. Although we are unaware of 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 6, 2024, Middleton became aware of suspicious activity within our computer network. We immediately took steps to secure our systems and launched an investigation into the nature and scope of the activity with the assistance of third-party forensic specialists. The investigation determined that an unauthorized actor accessed our systems at various periods of time from September 1, 2024, to September 8, 2024, and certain information contained within those systems was viewed or copied by the unknown actor. Middleton therefore undertook a comprehensive and time-intensive review of the data at risk to determine what information was potentially affected, and to whom that information related. Those efforts recently completed, and Middleton is notifying you because the investigation determined that certain information relating to you was contained within the impacted files.

What Information Was Involved? The following types of information related to you were found in the impacted files: your name, <<DATE ELEMENTS>>. Middleton 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. We take this event seriously, and the confidentiality, privacy, and security of information in our care is among our highest priorities. Upon learning of this event, we moved quickly to investigate and respond, assess the security of our network, and notify affected individuals. As part of our ongoing commitment to information security, we are also 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 they may take steps to best protect their information, should they feel it is appropriate to do so.

As an added precaution, we are offering you immediate access to credit monitoring and identity theft protection services for <<12/24>> months at no cost to you, through IDX. You can find information on how to enroll in these services in the enclosed *Steps You Can Take to 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 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 call 1-833-903-3648 from 8:00 a.m. CST to 8:00 p.m. CST, Monday through Friday, excluding major U.S. holidays. You may also write to us at PO Box 506 Bryant, AR 72089. We take this event very seriously and sincerely regret any inconvenience or concern this event may cause you.

Sincerely,

Middleton Heat & Air

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

1. Website and Enrollment. Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is May 6, 2025.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-903-3648 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Watch for Suspicious Activity. If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

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	1-800-916-8800
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 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.