EXHIBIT 1

This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, EnCon 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 August 21, 2025, EnCon was alerted to suspicious activity on our network and found certain systems were encrypted by malware. Upon being alerted to the suspicious activity, Encon moved quickly to bring systems offline, ensure the security of the network, and launch an investigation into the nature and scope of the event. The investigation determined that an unauthorized actor gained access to Encon's network between August 12, 2025 and August 21, 2025, and copied certain information off the network.

As part of the investigation, EnCon conducted a review of the information that was copied to determine what information was involved and to whom the information related. The review concluded on October 16, 2025 and determined that information related to individuals may be involved.

The information that could have been subject to unauthorized access includes name and Social Security number.

Notice to Nebraska Resident

On or about November 19, 2025 EnCon provided written notice of this incident to 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 discovering the event, EnCon moved quickly to investigate and respond to the incident, assess the security of EnCon systems, and identify potentially affected individuals. Further, EnCon notified federal law enforcement regarding the event. EnCon is also working to implement additional safeguards and training to its employees. EnCon is providing access to credit monitoring services for twelve (12) months, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, EnCon is providing impacted individuals with guidance on how to better protect against identity theft and fraud. EnCon 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. EnCon is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

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

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

Enrollment Code: <<XXXXXXXX>>

Enrollment Deadline: February 19, 2026

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:

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

November 19, 2025

NOTICE OF <<SECURITY INCIDENT/DATA BREACH>>

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

EnCon United Company and its subsidiaries and affiliates, including the one you work(ed) for, (collectively referred to as “EnCon”) writes to inform you of a recent event that may impact some of your information. The privacy and security of information in our care are among our highest priorities. While there is no evidence of actual or attempted fraud or identity theft in connection with this event, we are providing this notice in an abundance of caution to inform you of the event, our response, and steps that you can take to help protect your information, should you feel it necessary to do so.

What Happened?

On August 21, 2025, EnCon was alerted to suspicious activity on our network and found certain systems were encrypted by malware. Upon being alerted to the suspicious activity, Encon moved quickly to bring systems offline, ensure the security of the network, and launch an investigation into the nature and scope of the event. The investigation determined that an unauthorized actor gained access to Encon’s network between August 12, 2025 and August 21, 2025, and copied certain information off our network.

As part of the investigation, EnCon conducted a review of the information that was copied to determine what information was involved and to whom the information related. The review concluded recently and determined that your information was present within the impacted data.

What Information Was Involved?

The information related to you that was identified in the review includes your name and the following information: <<DATA ELEMENTS>>. Please note, there is no evidence of actual or attempted fraud or identity theft in connection with this event.

What We Are Doing.

EnCon takes this event seriously and the security, privacy, and confidentiality of the information in our care are among our top priorities. Upon learning of the event, we quickly took steps to contain the suspicious activity in our network and investigate what happened. We also notified federal law enforcement. As part of our ongoing commitment to information security, we are reviewing our policies, procedures, and security protocols to reduce the likelihood of a similar event occurring in the future.

As an added precaution, EnCon is also offering you access to enroll in <<12/24>> months of complimentary credit monitoring through a third-party provider called IDX. You must enroll in these services yourself, as EnCon cannot do so on your behalf. Enrollment instructions can be found in the enclosed *Steps You Can Take to Help Protect Personal Information* below.

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. Incidents of suspected identity theft should be promptly reported to law enforcement or other relevant authorities. Please review the enclosed *Steps You Can Take to Help Protect Personal Information*, which includes further information on what you can do to protect your information against misuse, should you feel it necessary to do so. Additionally, EnCon encourages you to enroll in the complimentary credit monitoring services.

For More Information.

Encon understands that you may have questions that are not addressed by this letter. Should you have any additional questions, please reach out to our dedicated assistance line at 1-833-788-9712. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. You may also write to EnCon at 2140 South Ivanhoe Street, Suite 100, Denver, Colorado 80222.

Sincerely,

EnCon United Company

STEPS YOU CAN TAKE TO HELP 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 February 19, 2026.

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 1-833-788-9712 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, 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, 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 New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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. We encourage consumers to review their 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.

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

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.