EXHIBIT 1

By providing this notice, Central McGowan ("Central") 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 or about January 11, 2025, Central became aware of suspicious activity related to certain computer systems. Upon learning of the suspicious activity, Central immediately took steps to secure their systems and launched an investigation into the nature and scope of the activity. The investigation determined that there was unauthorized access to certain systems within Central's network at various times between January 8, 2025 and January 10, 2025, and certain information contained within the network was viewed or copied by an unauthorized actor during that time.

Upon becoming aware of these findings, Central undertook a comprehensive and time-intensive review of the data potentially at risk to determine what information was potentially affected, and to whom that information related. Those efforts recently completed, and Central provided notice to individuals whose personal information was contained within the potentially impacted files.

The information that could have been subject to unauthorized access includes name, Social Security number, date of birth, driver's license number, passport number, employer ID, financial account information, electronic signature, and health insurance information.

Notice to Nebraska Residents

On or about July 1, 2025, Central began providing written notice of this incident to approximately two (2) Nebraska residents. 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, Central moved quickly to investigate and respond to the same, assess the security of Central systems, and identify potentially affected individuals. Further, Central notified federal law enforcement regarding the event. Central is also working to implement additional safeguards and training to its employees. Central also provided access to credit monitoring services for one year through Epiq to all employees, at no cost to these individuals.

Additionally, Central is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Central 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.

Central is also providing written notice of this incident to relevant state regulators, as required, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

Central McGowan, Inc
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

P
[redacted]

000010102G0400

P

July 1, 2025

NOTICE OF SECURITY INCIDENT

Dear [redacted]:

Central McGowan Inc. ("Central") writes to inform you of a recent event that may affect the privacy of some of your information. Although we are unaware of any identity theft or fraud in relation to the 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 or about January 11, 2025, Central became aware of suspicious activity related to certain computer systems. Upon learning of the suspicious activity, we immediately took steps to secure our systems and launched an investigation into the nature and scope of the activity. The investigation determined that there was unauthorized access to certain systems within our network at various times between January 8, 2025 and January 10, 2025, and certain information contained within our network was viewed or copied by an unauthorized actor during that time. Upon becoming aware of these findings, we undertook a comprehensive and time-intensive review of the data potentially at risk to determine what information was potentially affected, and to whom that information related. Those efforts recently completed, and Central is notifying you because the investigation determined that certain information relating to you was contained within the potentially impacted files.

What Information Was Involved? The following types of information related to you were found in the potentially impacted files: your name, Social Security number, date of birth, driver's license number, Passport number, employer assigned identification number, financial account information, electronic signature, and health insurance information. Please note that at this time Central is not aware of any identity theft or fraud in relation to this event.

What We Are Doing. We take this event seriously, and the confidentiality, privacy, and security of information in our care are 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. We also took steps to further enhance our network security to attempt to ensure the privacy of the data on our network. As part of our ongoing commitment to information security, we are also reviewing existing security policies and dedicating significant resources to implement 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.

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. Additional information regarding resources available to you can also be found in the enclosed *Steps You Can Take to Help Protect Your Information*.

For More Information. We understand that you may have questions about this event that are not addressed in this [redacted], between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays.

Sincerely,

Central McGowan, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

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.

P 0000102028000

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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately [#] Rhode Island residents that may be impacted by this event.