EXHIBIT 1

Amtech is providing notice to your office, on behalf of certain other customer data owners, of an event that may affect personal information relating to four (4) Maine residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Amtech does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about April 7, 2025, Amtech identified suspicious activity on its computer network. In response, Amtech took steps to secure the network and began a comprehensive investigation to determine what occurred. The investigation determined that between March 11 and April 7, 2025, certain files were potentially copied from the network as part of a cyber event. As a result of that determination, Amtech initiated a comprehensive review of the relevant files to determine what type of information was present, and to whom the information was related. This review identified personal information of individuals associated with certain Amtech customers. Amtech notified the relevant customers and, thereafter, worked with its customers to notify potentially impacted individuals. The information related to Maine residents that was present in the reviewed files included name, Social Security number, and date of birth.

Notice to Maine Residents

On or about August 29, 2025, Amtech provided written notice of this event, on behalf of certain customers, to four (4) Maine 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

Amtech took prompt steps to secure its system and conduct a diligent investigation into the nature and scope of this event. Amtech notified relevant customers and worked with those organizations to provide notice to potentially impacted individuals. Further, while Amtech does have safeguards in place to protect information in its care, as part of its response to this matter, it is reviewing its policies and its technical security measures.

Additionally, Amtech is providing impacted individuals with guidance on how to better protect against identity theft and fraud, as demonstrated in the attached ***Exhibit A***. Amtech is also providing Maine residents with access to credit monitoring services for one (1) year, through TransUnion, at no cost as part of its notification to individuals. Amtech is providing written notice of this event to relevant state regulators, as necessary. Further, Amtech notified federal law enforcement regarding the event.

EXHIBIT A

Amtech Software, Inc.
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS1567

0004737

20_0004737

[redacted]

August 29, 2025

Notice of Data Breach

Dear [redacted]:

Amtech Software, Inc. ("Amtech") is writing to make you aware of an event that may affect some of your information. This notice provides information about the event, our response, and resources available to you to help protect your information, should you feel it appropriate to do so. Amtech has your information because we provided an integrated payroll product to [redacted].

What Happened? On or about April 7, 2025, we became aware of suspicious activity on our computer network. In response, we immediately took steps to secure the network and began a comprehensive investigation. The investigation determined that, between March 11, 2025 and April 7, 2025, certain files were potentially copied from the network as part of a cyber incident. Amtech undertook a thorough review of the relevant files to determine what information was present, and to whom the information related. You are receiving this notice because your information was found in the relevant files.

What Information Was Involved? Our investigation determined the following information related to you was contained in the files: name, date of birth and Social Security number.

What We Are Doing. In response to this incident, we promptly took steps to secure our network, conduct a thorough investigation, review the content of relevant data for sensitive information, and notifying potentially affected individuals. As an added precaution, we are offering you access to 12 months of complimentary credit monitoring and identity theft protection services through TransUnion. If you wish to activate these services, you may follow the instructions included in the enclosed ***Steps You Can Take To Help Protect Personal Information***.

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. We also encourage you to review the information contained in the enclosed ***Steps You Can Take To Help Protect Personal Information*** and enroll in the credit monitoring services we are offering. Please note, due to privacy restrictions, we are unable to automatically enroll you in the complimentary monitoring services, if you wish to receive the monitoring services, you must follow the enrollment instructions in this letter.

For More Information. If you have questions, please contact our dedicated assistance line at 1-833-426-7050 Monday through Friday, from 8:00a.m. to 8:00 p.m. Eastern, excluding Major U.S. Holidays. You may also write to us at Amtech Software, Inc., 600 W Office Center Drive, Suite 350, Fort Washington, PA 19034.

Sincerely,

Amtech Software, Inc.

Steps You Can Take To Help Protect Personal Information

Enroll in Monitoring Services

In response to this matter, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months 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 the 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 enroll in Credit Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted, please provide the following unique code to receive services: [redacted].

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. 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.

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 their 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 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/. You may also contact Amtech Software, Inc., at 600 W Office Center Drive, Suite 350, Fort Washington, PA 19034 or call us at 215-639-9540.

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. NW, 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; and 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; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 3 Rhode Island residents that may be impacted by this event.