EXHIBIT 1

By providing this notice, Asplundh Engineering Services, LLC (formerly Kupper Engineering LLC) ("Asplundh Engineering") 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 around January 18, 2026, Asplundh Engineering identified suspicious activity on their computer network. Upon becoming aware of this activity, Asplundh Engineering quickly took steps to secure the environment, with the assistance of third-party specialists, and launched an investigation into the nature and scope of the activity. The investigation determined that an unauthorized actor accessed their network at various times between approximately January 11, 2026 and January 17, 2026 and, during that period, accessed and copied certain files and information from the network. Upon identifying this information, Asplundh Engineering began a comprehensive and time-intensive review of the involved files to determine whether anything sensitive was potentially accessed and to whom the information related. That review was recently completed, and Asplundh Engineering provided notification to individuals whose information was contained within the impacted data.

While the information that could have been subject to unauthorized access varies by individual, the information potentially impacted for the one involved Maine resident includes name and driver's license number.

Notice to Maine Resident

On or about June 4, 2026, Asplundh Engineering provided written notice of this incident to approximately one (1) Maine 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, Asplundh Engineering moved quickly to investigate and respond to the same, assess the security of Asplundh Engineering systems, and identify potentially affected individuals. Asplundh Engineering is also working to implement additional safeguards and training to its employees. Asplundh Engineering is providing access to credit monitoring services for twelve (12) months, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

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

Asplundh Engineering is also providing written notice of this incident to relevant state regulators, where required.

EXHIBIT A

Asplundh Engineering Services, LLC
c/o Cyberscout
PO Box 245
Bellmawr, NJ 08099

June 4, 2026

Dear :

Asplundh Engineering Services, LLC (successor by merger to Kupper Engineering, LLC) ("Asplundh Engineering") writes to inform you of an event that may affect the privacy of some of your information. Although we are unaware of any identity theft occurring as a result of this event, we are providing you with information about the event, our response, and steps you may take to help protect your information, should you feel it appropriate to do so.

What Happened? On or around January 18, 2026, Asplundh Engineering identified suspicious activity on our computer network. Upon becoming aware of this activity, we quickly took steps to secure the environment, with the assistance of third-party specialists, and launched an investigation into the nature and scope of the activity. The investigation determined that an unauthorized actor accessed our network at various times between approximately January 11, 2026 and January 17, 2026 and, during that period, accessed and copied certain files and information from our network. Upon identifying this information, Asplundh Engineering began a comprehensive and time-intensive review of the involved files to determine whether anything sensitive was potentially accessed and to whom the information related. That review recently completed, and we are providing you with notification upon determining that your information was contained within the impacted data.

What Information Was Involved? The information contained in the impacted data included your name and the following information: date of birth, employer assigned identification number, and Social Security number. At this time, we have no evidence that your information was used to commit identify theft or fraud as a result of this event

What We Are Doing. Asplundh Engineering takes the confidentiality, privacy, and security of information in our care very seriously. Upon learning of the event, we moved quickly to investigate and respond, assess the security of our network, and notify affected individuals. Asplundh Engineering also implemented additional security measures to further protect against similar events in the future. We are also offering you access to complimentary credit monitoring and identify theft protection services through Cyberscout, a Transunion company for 12 months. More information on how to enroll in this complimentary service can be found in the enclosed *Steps You Can Take to 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, monitoring your free credit reports for suspicious activity, and reporting any suspected identity theft to your financial institution. Please review the enclosed *Steps You Can Take to Protect Personal Information*, which contains information on what you can do to better safeguard against possible misuse of your information. You may also enroll in the complimentary credit monitoring services we are offering to you.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call 1-800-405-6108. This line is available 8am – 8pm ET Monday to Friday, excluding major U.S. holidays. You may also write to us at 300 Brookside Ave. Bldg. 14 Ambler, PA 19002.

Sincerely,

Asplundh Engineering Services

0000210020001

Steps You Can Take To Protect Personal Information

Enroll in Monitoring 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: . 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 one-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 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.