CONSTANGY
Brooks Smith & Prophete

Aubrey Weaver, Partner
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, PA 19103
aweaver@constangy.com
Direct: 215.770.4234

October 22, 2026

VIA U.S. MAIL
Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

RECEIVED
OCT 30 2026
CONSUMER PROTECTION

RE: Notice of Data Security Incident

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP represents Allied Machine & Engineering Corp. ("AMEC") in connection with a recent data security incident described below. AMEC is in the process of notifying affected individuals of the incident. The purpose of this letter is to provide notice to your office pursuant to N.H. Rev. Stat. § 359-C:20.

I. NATURE OF THE SECURITY INCIDENT

AMEC learned of unusual activity involving its network environment in September 2026. In response, AMEC took measures to investigate with the assistance of external experts. That investigation revealed that some data could have been acquired without authorization in connection with the event. AMEC thereafter undertook a comprehensive review of the potentially affected information and worked to gather information needed to provide notice. This process concluded on September 29, 2026, at which time AMEC arranged to provide notification.

II. NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

On October 22, 2026, AMEC notified one (1) New Hampshire resident of the incident via USPS First-Class Mail. A sample copy of the notification letter sent to the impacted residents is included with this correspondence.

The potentially affected personal information may have included individuals' names and Social Security numbers. The notification letters include an offer of complimentary credit monitoring and identity protection services through Kroll.

III. ACTIONS TAKEN IN RESPONSE TO THE INCIDENT

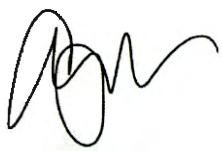
As soon as AMEC discovered the unusual activity, it took immediate steps to secure its network environment, launched an investigation with the assistance of independent experts, and worked to determine whether any personal information was accessed or acquired without authorization in connection with the incident. AMEC thereafter worked diligently to determine what personal

information may have been affected, the individuals to whom the information pertained, and the addresses for those individuals to provide appropriate notification.

IV. CONTACT INFORMATION

If you have any questions or need additional information, please do not hesitate to contact me at 215.770.4234 or aweaver@constangy.com.

Sincerely,



Aubrey Weaver
Partner, Cybersecurity & Data Privacy Team

Encl. Sample Consumer Notification Letter

ALLIED MACHINE & ENGINEERING

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

KROLL

SCAN TO ENROLL

Subject: Notice of Data Seeurity Incident

<<Date>> (Format: Month Day, Year)

Dear <<First_Name>> <<Last_Name>>,

We are writing to inform you of a recent data security incident that potentially involved your information. Allied Machine & Engineering Corp. takes the privacy and security of all information in our possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your information.

What Happened. We recently learned that some of your personal information was involved in a data security incident. We experienced unusual activity involving our network systems on September 14, 2026, and immediately started an investigation using independent experts to assist. We later learned that some data could have been accessed or acquired without authorization in connection with the activity. We then worked to determine what information was potentially involved in the incident and gathered contact information needed to provide notice. This process concluded on September 29, 2026.

What Information Was Involved. The potentially involved information may have included your name and Social Security number.

What We Are Doing. As soon as we discovered the incident, we took the steps described above. As part of our ongoing commitment to information security, we are reviewing existing policies and procedures and implementing enhanced security measures to reduce the likelihood of a similar incident occurring in the future. We are further notifying you of this event and advising you about steps you can take to help protect your information.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for <<ServiceTerminMonths>> months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Coverage can reimburse individuals for certain eligible losses associated with identity theft recovery, such as those listed below. Individuals must activate their monitoring services during the Activation Period to be eligible for insurance coverage. The policy provides reimbursement, up to $1,000,000 USD with a $0 deductible, from an A.M. Best "A-rated" carrier. Potential covered expenses include:

– Lost wages or income

– Attorney and legal fees

– Expenses incurred for refiling of loans, grants, and other lines of credit

– Costs of childcare and/or elderly care incurred as a result of identity restoration

– Unauthorized Electronic Funds Transfers (EFT)

– Privacy Investigator costs

– Funds stolen from a financial institution including:

- Traditional credits, pre-paid credit cards, and debit card deductibles
- Unauthorized electronic fund transfer from a personal account

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (Date)>> to activate your identity monitoring services.

Membership Number: **<<Member ID (S_N)>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is included with this letter.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the complimentary services offered to you through Kroll by using the enrollment code provided above.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call (844) 301-0363 Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Please be assured that we take the privacy and security of all information within our possession very seriously. We hope you will accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Allied Machine & Engineering Corp.
120 Deeds Drive
Dover, Ohio 44622

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

California Attorney General
1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
https://oag.maryland.gov
888-743-0023

New York Attorney General
The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

New York Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.