Return Mail Processing
PO Box 999
Suwanee, GA 30024

2 1 501 **********ALL FOR AADC 945
SAMPLE A. SAMPLE - L04
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

February 3, 2025

RE: Important Security Notification. Please read this entire letter.

Notice of Data Breach

Dear Valued Employee or Former Employee:

SMC Corporation of America ("SMC") was the victim of a cybersecurity incident that may affect the security of your personal information. You are receiving this letter because you are a current or former employee of Advanced Pressure Technology ("APTech"), a subsidiary of SMC. This letter will provide you with information about the incident, steps we are taking in response, and steps you may take to guard against identity theft and fraud, should you feel it is appropriate to do so.

What Happened? On or around December 8, 2024, SMC discovered that it had experienced a cybersecurity incident. A foreign cyber threat actor attempted to disrupt SMC's IT infrastructure in a possible effort to deploy ransomware and solicit a ransom payment from SMC (the "Incident"). SMC's continuing investigation of the Incident determined that the threat actor gained unauthorized access to SMC's technology infrastructure, allowing them to access certain personal information on current or former SMC employees, or SMC affiliated employees, located in the U.S. and Canada. The Incident was discovered expeditiously, cyber security experts were retained, and security measures were implemented to contain the Incident.

What Information Was Involved? The information potentially exposed may have included APTech employment data, which could include sensitive personal information, such as: first and last name, date of birth, address, bank account information, driver's licenses, certain payroll information, SMC employee account number and position, Social Security Number, SMC employee benefit information, data related to certain medical information in connection with SMC benefits, and other identifying information.

We are providing this notification because your personal information may have been exposed as part of SMC's security incident; however, an investigation is still ongoing to determine the full extent of the Incident. To date, SMC is unaware of any misuse (or attempted misuse) of your personal information for identity theft or fraud stemming from the Incident.

What Are We Doing? As soon as we learned of this situation, SMC's IT Department quickly identified the threat, took action to block unauthorized users from accessing SMC's systems and launched an investigation. SMC engaged cyber security experts to investigate and attempt to resolve the Incident. This investigation is still ongoing as we are working with law enforcement to bring the threat actors behind this to justice.

While SMC has made several significant investments in its cyber security systems, today's environment demands constant refinement and diligence. SMC is working with its IT team and cyber security partner to constantly evaluate security protocols and processes to prevent future incidents.

What Actions You Can Take? As always, we recommend that you be on the alert for suspicious activity related to your financial accounts and credit reports. We encourage you to regularly monitor your statements and records to ensure there are no transactions or other activities that you did not initiate or authorize. You should report any suspicious activity to the appropriate service provider. If you observe unusual activity on any debit/credit card, or you believe your personal bank account shows signs of compromise, we advise you to close out those accounts and request new cards and account credentials.

Additionally, citizens of the U.S. should report incidents of suspected identity theft to your local law enforcement, the Federal Trade Commission (the "FTC"), and your state attorney general. To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (1 (877) 438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. Information on how to contact your state attorney general can be found below:

Attorney General Rob Bonta
California Attorney General's Office
1300 "I" Street
Sacramento, CA 95814-2919
Phone: (916) 445-9555
https://oag.ca.gov/contact

Additional Office Locations:

Office of the Attorney General
455 Golden Gate, Suite 11000
San Francisco, CA 94102-7004
Phone: (415) 510-4400

Office of the Attorney General
2550 Mariposa Mall, Room 5090
Fresno, CA 93721-2271
Phone: (559) 705-2300

Office of the Attorney General
300 South Spring Street
Los Angeles, CA 90013-1230
Phone: (213) 269-6000

Office of the Attorney General
1515 Clay Street
Oakland, CA 94612-1499
Phone: (510) 879-1300

Office of the Attorney General
600 West Broadway Street, Suite 1800
San Diego, CA 92101-3702
Phone: (619) 738-9000

Please take advantage of additional free resources for identity theft. We recommend that you review the tips provided by the FTC's Consumer Information website, a valuable resource with helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacyidentity-online-security. A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, is on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

Additionally, under the Fair Credit Reporting Act, as a U.S. citizen, you have the right to know what is in your file and receive notification if information in your file has been used against you in applying for credit or other transactions. All consumers are entitled to one free disclosure every 12 months upon request from each nationwide credit bureau and from nationwide specialty consumer reporting agencies. See www.consumerfinance.gov/learnmore for additional information.

Placing a Security Freeze

Any consumer may place a free security freeze on their credit report by: (i) requesting one in writing by certified mail to the consumer reporting agency, (ii) calling the agency directly, or (iii) submitting a form online directly to the agency. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. Please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services. We recommend that you work with potential lenders, employers and service providers to ensure that you are protecting both your information and the approval status of your applicable request.

To place a security freeze on your credit reports, you must contact each of the following major consumer reporting agencies: Equifax (www.equifax.com); TransUnion (www.transunion.com); and Experian (www.experian.com), at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
(888) 298-0045
https://www.equifax.com/personal/credit-report-services/credit-freeze/

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 160
Woodlyn, PA 19094-2000
(888) 909-8872
https://www.transunion.com/credit-freeze

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
(888) 397-3742
https://www.experian.com/freeze/center.html

The credit reporting agencies have a certain number of days after receiving your request to place a security freeze on your credit report, so we recommend placing the freeze as soon as you possibly can. The credit bureaus must also send written confirmation to you, and may provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or temporary lifting of the security freeze.

Lifting or Suspending a Security Freeze

To temporarily lift or suspend the security freeze, you must call, make a request online, or send a request via electronic media to the credit reporting agencies and include proper identification (name, address, and social security number) and the PIN number (if provided) or password provided to you when you placed the security freeze. Please note, your state may not allow this action to be completed. You should always check your state's laws on credit freezing before placing a freeze on your credit report.

Removing a Security Freeze

To remove the security freeze, you can either submit the request online, or send a written request to each of the three credit bureaus by mail, secure electronic method, or via their online form, and include proper identification (name, address, and social security number) and the PIN number (if provided) or password provided to you when you placed the security freeze.

Credit Monitoring

Although we do not have any evidence that your personal information has been misused for identity theft or fraud, out of an abundance of caution, SMC is providing Experian IdentityWorks^{SM} credit monitoring services for **24 months** at no cost to you.

If you believe there was fraudulent use of your information as a result of this Incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the Incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for **24 months** from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.
While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by May 30, 2025** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bplus
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this Incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-833-918-9829 by **May 30, 2025**. Be prepared to provide engagement number [redacted] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

For More Information. We regret and apologize for any inconvenience this may cause you. If you have further questions or concerns, or would like an alternative to enrolling online, please call 1-833-918-9829 toll-free **Monday through Friday from 9 a.m. – 9 p.m. Eastern** (excluding major U.S. holidays). Be prepared to provide your engagement number [redacted].

Thank you for your immediate attention to this situation, as well as your understanding in the short-term. Our cyber security, as well as the safety and stability of our employees, current, former, and future, is of the utmost importance to us.

We will advise you of any relevant or necessary updates as they become available. Again, we sincerely apologize for any impact this Incident has caused.

Sincerely,

Kelley L. Stacy
Director & Executive Officer
SMC Corporation (Japan)

President, CEO
SMC Corporation of America

SMC Corporation of America
10100 SMC Blvd.
Noblesville IN 46060, U.S.A.

Advanced Pressure Technology
687 Technology Way
Napa, CA 94558 U.S.A.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions