CONSTANGY
BROOKS, SMITH &
PROPHETE LLP

March 2, 2023

VIA ELECTRONIC MAIL
Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: **Notice of Data Security Incident**

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP ("Constangy") represents HTI Technology & Industries, Inc. ("HTI"), a leading manufacturer of mechatronic devices based in Lavergne, Tennessee. We are writing to notify you of data security incident experienced by HTI which is described in greater detail below.

Nature of the Security Incident

On August 22, 2022, staff members of one of HTI's wholly-owned subsidiaries reported having difficulty accessing certain systems within the network. HTI immediately took steps to ensure the environment was secure and engaged an independent cybersecurity firm to conduct a forensic investigation. According to that investigation, an unauthorized actor gained access to the HTI subsidiaries' environment between August 18 and August 22, 2022 and potentially accessed and/or downloaded certain files. HTI then enlisted a third-party vendor to comprehensively review the potentially impacted data to confirm whether personal information was involved and determine the identities of any individuals who may have been affected. As soon as that review concluded, HTI worked diligently to collect up-to date mailing addresses for purposes of notification. HTI completed those efforts on February 24, 2023 and arranged for notification letters to be sent as soon as possible.

The potentially impacted information may have included names as well as Social Security number. To date, HTI has no evidence of the successful or attempted misuse of any of this information.

Number of New Hampshire Residents Involved

On March 2, 2023, HTI will be notifying one (1) New Hampshire resident of this incident via U.S. First-Class Mail. A sample copy of the notification letter being sent to the impacted individual is included with this correspondence.

Steps Taken to Address the Incident

HTI has implemented additional security measures in its environment to reduce the risk of a similar incident occurring in the future. HTI also reported the incident to the Federal Bureau of Investigation and will cooperate with any resulting investigation. In addition, out of an abundance of caution, HTI is providing notified individuals with complimentary credit monitoring and identity protection services along with additional resources to assist them. HTI has also established a toll-free call center to address any questions and to help individuals resolve issues if their identity is compromised due to this incident.

Contact Information

HTI remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at or

Sincerely,

David McMillan of
Constangy, Brooks, Smith & Prophete, LLP

Enclosure: Sample Notification Letter

Return to IDX:
10300 SW Greenburg Rd.
Suite 570
Portland, Oregon 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

<< First Name>> << Last Name>>
<<Address1>>, <<Address2>>
<<City>>, <<State>> <<Zip>>

March 2, 2023

Re: Notice of Data <<Variable Text 1: Breach or Security Incident>>

Dear << First Name>> << Last Name>>:

I am writing to notify you of a data security incident experienced by HTI Technology & Industries, Inc. ("HTI") which may have affected your personal information. HTI operates in the U.S. as HTI Technology, American Control Electronics, Klauber Machine and Gear, GOT Interface, AllMotion, Tru Vu Monitors and Global Point Technology. Please read this letter carefully as it contains important details about the incident and resources you may utilize to help protect your information. HTI takes this matter extremely seriously as the security of our networks and the information we store is of paramount importance.

What Happened? On August 22, 2022, staff members of one of HTI's wholly-owned subsidiaries reported observing unusual activity in the network, including difficulty accessing certain systems. We immediately began to investigate the issue and took steps to ensure that our environment was secure. We also engaged independent cybersecurity experts to conduct a forensic investigation in order to determine what happened and whether any sensitive data was impacted as a result. That investigation determined that between August 18 and August 22, 2022, an unauthorized actor gained access to our subsidiaries' environment and potentially accessed and/or downloaded certain files, some of which may have contained personal information. We then immediately undertook a comprehensive review process to discern the precise nature of the potentially impacted data and the individuals who may have been affected, and worked to identify current mailing addresses for purposes of notification. We completed those efforts on February 24, 2023 and arranged for notification letters to be sent as soon as possible.

What Information was Involved? Based on our review of the potentially impacted data, we believe that your name as well as your <<Variable Text 2 – Data Elements>> may have been affected. Please note that HTI has no evidence that this information has been misused.

What Are We Doing? As soon as we learned of the incident, we immediately took steps to secure our network and enlisted a leading cybersecurity firm to conduct a forensic investigation. We also reported the incident to the FBI and will provide whatever cooperation is necessary to help hold the perpetrator(s) accountable. Since the incident, we have implemented additional security measures in our environment to minimize the risk of a similar event happening again.

HTI is also offering you <<12 / 24>> months of complimentary identity protection services through IDX, a data breach and recovery services expert. These services include credit[1] and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity recovery services. To enroll, please call IDX at 1-800-939-4170 or visit https://app.idx.us/account-creation/protect and reference the enrollment code above. Please note that the deadline to enroll is June 2, 2023.

[1] To receive credit monitoring 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.

What You Can Do: We encourage you to enroll in the complimentary services from IDX. In addition, following this letter is a pamphlet with additional resources you may utilize to help protect your information. We recommend that you read this pamphlet carefully and take advantage of these resources if you have any concerns.

For More Information: If you have any questions or need assistance, please call IDX at 1-800-939-4170. IDX representatives are available from 8:00 A.M. to 8:00 P.M. Central Time, Monday through Friday (excluding holidays). IDX call center representatives are fully versed on this incident and can answer any questions that you may have.

Please accept my sincere apologies and know that HTI takes this matter very seriously and deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

Jon Seago, Chief Financial Officer
HTI Technology & Industries, Inc.

Steps You Can Take to 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 (FTC).

Request a Copy of Your 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 https://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 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Place a 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 https://www.annualcreditreport.com.

Put a 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 (FTC)
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

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 https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.