Maria Efaplomatidis
77 Water Street Suite 2100
New York, NY 10005
Maria.efaplomatidis@lewisbrisbois.com

LEWIS BRISBOIS BISGAARD & SMITH LLP

May 25, 2022

Via Email

Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

To Whom It May Concern,

Lewis Brisbois Bisgaard & Smith LLP ("Lewis Brisbois") represents Gerber Technology, LLC ("Gerber") in connection with a recent data security incident described in greater detail below.

1. **Nature of the security incident.**

On February 16, 2022, Gerber Technology discovered that it had experienced an incident disrupting access to certain of its systems. In response, Gerber Technology took immediate steps to secure its systems and promptly launched an investigation. In so doing, Gerber Technology engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. On March 25, 2022, Gerber Technology learned that personal information may have been impacted in connection with the incident which is the reason for this notification. Please note that Gerber Technology has no evidence of the misuse or attempted misuse of any potentially impacted information. Gerber Technology reviewed their records and on April 26, 2022, identified all persons impacted in the incident and verified their contact information.

The information that may have been accessible by the malicious actor(s) responsible for this incident includes first names as well as social security numbers, driver's license information, passport number, and bank account information.

2. **Number of New Hampshire residents affected.**

Gerber notified thirty-two New Hampshire residents of this incident via first class U.S. mail on May 24, 2022. A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the Incident.

As soon as Gerber discovered this incident, Gerber notified the Federal Bureau of Investigation and took steps to secure its systems and launched an investigation to determine what happened and whether personal information had been accessed or acquired without authorization. Gerber has also implemented additional safeguards to help ensure the security of its systems and to reduce the risk of a similar incident occurring in the future.

Gerber has established a toll-free call center through Kroll, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. In addition, while Gerber is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, Gerber is also providing complimentary identity protection services to notified individuals.

4. Contact information.

Gerber remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Lewis Brisbois.

Best regards,

Maria Efaplomatidis of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Sample Notification Letter

LECTRA

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1 ("Subject: Notice of Data" [Breach / Security Incident])>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing to inform you of a recent data security incident experienced by Gerber Technology LLC that may have affected your personal information. Gerber Technology LLC takes the privacy and security of all personal information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened? On February 16, 2022, Gerber Technology LLC discovered that it had experienced an incident disrupting access to certain of its IT systems. In response, Gerber Technology LLC took immediate steps to secure its systems and promptly launched an investigation. In so doing, Gerber Technology LLC engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. On March 25, 2022, Gerber Technology LLC learned that personal information may have been impacted in connection with the incident which is the reason for this notification. Gerber Technology reviewed their records and on April 26, 2022, identified all persons impacted in the incident and verified their contact information.

What Information Was Involved? The information potentially impacted in connection with this incident included your name as well as your Social Security number, driver's license information, passport number, and bank account information.

What Are We Doing? As soon as Gerber Technology LLC discovered this incident, Gerber Technology LLC took the steps described above. In addition, Gerber Technology LLC implemented measures to enhance the security of its digital environment in an effort to minimize the risk of a similar incident occurring in the future. Gerber Technology LLC also notified law enforcement of this incident and has been and will continue to provide whatever cooperation is necessary to assist in their investigation. Out of an abundance of caution, Gerber Technology LLC is providing you with information about steps that you can take to help protect your personal information and is offering you complimentary identity monitoring services for 24 months through Kroll. 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, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

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: **<<Membership Number 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. Gerber Technology LLC also encourages you to activate the complementary services being offered to you through Kroll.

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 Kroll at XXX-XXX-XXXX from 8:00 A.M. to 5:30 P.M. Central Time, Monday through Friday (excluding holidays). Kroll call center representatives are available to help answer any questions you may have.

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

Sincerely,

Karen Gibbs, CPA, CGMA - Deputy Chief Financial Officer
Gerber Technology LLC

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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$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.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

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.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR 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).

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 http://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

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 http://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, 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.