muRata
INNOVATOR IN ELECTRONICS

Via E-Mail

Attorney General Formella
Office of the Attorney General
1 Granite Place South
Concord, NH 03301
Phone Number: 603- 271-3658
Fax: 603- 271-2110
DOJ-CPB@doj.nh.gov

Re: Cybersecurity Incident Involving Murata Electronics North America, Inc.

Dear Attorney General Formella:

I am writing on behalf of Murata Electronics North America, Inc. ("Murata"), a company located at 3330 Cumberland Blvd., SE, Suite 700, Atlanta, GA 30339, with respect to a recent cybersecurity incident that was first discovered by Murata on February 28, 2026 (hereinafter, the "Incident"). Murata takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of New Hampshire residents being notified, and the steps that Murata has taken in response to the Incident. We have also attached a sample of the notification to be made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of the Incident

On February 28, 2026, Murata discovered that unauthorized access by a third party within the IT environment occurred between March 2025 and February 28, 2026. Murata immediately excluded external access to its network and promptly engaged a specialized third-party cybersecurity firm to assist with securing the environment, and to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. At this time, there is no evidence that the potentially impacted information was misused by third parties.

Although Murata is unaware of any fraudulent misuse of information, it is possible that individuals' full name, address, email address, citizenship and marital status, social security numbers, driver's license and passport information, insurance policy information, health or medical condition related information, and financial account numbers may have been exposed and acquired as a result of this unauthorized activity.

2. Number of New Hampshire Residents Affected

Murata identified and notified one (1) resident of New Hampshire potentially affected by this Incident. A notification letter to this individual will be mailed on May 1st, 2026, by first class mail. A sample copy of the notification letter is included with this letter.

muRata
INNOVATOR IN ELECTRONICS

3. Steps Taken in Response to the Incident

Murata is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, Murata moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. Specifically, Murata engaged a specialized cybersecurity firm to assist with conducting an investigation to identify the nature and scope of the Incident, including identifying the potentially affected individuals. The investigation lasted between March 1, 2026 and April 6, 2026. Additionally, Murata reinforced its security system by restricting access to its network, forced password resets, and improved password management. Lastly, upon identifying the potentially impacted individuals, Murata began preparing for the delivery of notifications.

Although Murata is not aware of any actual or attempted misuse of the affected personal information, Murata offered 24 months of complimentary credit monitoring and identity theft restoration services through Kroll to all individuals to help protect their identity. Additionally, Murata provided guidance on how to better protect against identity theft and fraud, including providing 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 the contact details for the Federal Trade Commission.

4. Contact Information

Murata remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at patrick.garrett@murata.com or 469-691-0029.

Best regards,

/s/ Patrick Garrett

Patrick Garrett
Sr. Manager – Information Security & Privacy
Murata Electronics North America, Inc.
3330 Cumberland Blvd SE Suite 700
Atlanta, GA 30339

<<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>>

SCAN TO ENROLL

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

Notice of Data Breach

Dear <<First_name>> <<Last_name>>,

Murata Electronics North America, Inc. ("Murata") is writing to inform you of a recent data security incident that may have resulted in an unauthorized access to, or acquisition of, your sensitive personal information. While we are unaware of any fraudulent misuse of your personal information at this time, out of an abundance of caution, we are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

What Happened?

On February 28, 2026, Murata discovered that unauthorized access by a third party within the IT environment occurred between March 2025 and February 28, 2026. Murata immediately blocked external access to the network and promptly engaged a specialized third-party cybersecurity firm to assist with securing the environment, and to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The investigation lasted between March 1, 2026 and April 6, 2026. At this time, there is no evidence that your information was misused by third parties.

What Information Was Involved?

To date, although Murata has no evidence that any sensitive information has been misused by third parties as a result of this incident, we are notifying you out of an abundance of caution. Based on the investigation, it was determined that Murata's HR system was not impacted, however personal files owned by you, which were saved in a Murata account, may have been subject to unauthorized access or acquired. Your files may contain sensitive personal information which may include: names, address, email address, citizenship and marital status, social security numbers, driver's license and passport information, insurance policy information, health or medical condition related information, and financial account numbers.

What We Are Doing

Data privacy and security is among Murata's highest priorities. Murata is committed to doing everything it can to protect the privacy and security of the personal information in its care. Since the discovery of the incident, Murata moved quickly to investigate, respond, and confirm the security of its systems. Furthermore, Murata enhanced its security measures, and took steps, and will continue to take steps, to mitigate the risk of future harm.

In light of the incident, to help relieve concerns we have secured the services of Kroll to provide identity monitoring at no cost to you for 24 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. When enrolled in the service, 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. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or provide assistance in event that you become a victim of fraud. While Murata is covering the cost of these services, you will need to complete the activation process by following the instructions at the section "What You Can Do" below.

What You Can Do

Murata encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert or freeze on your credit file. You should also change passwords to your accounts and be aware of phishing attempts. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

You may also activate the identity monitoring services we are making available to you at no cost. To activate your identity monitoring service, you will need to follow the steps described below.

1. You must activate your identity monitoring services by ***<<b2b_text_6 (activation deadline)>>***. Your Activation will not work after this date.
2. Visit **https://enroll.krollmonitoring.com** to activate your identity monitoring services.
3. Provide Your Membership ID: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com. Identity Fraud Loss Reimbursement coverage is subject to the conditions and exclusions in the policy. Once activated the identify services will be active for 24 months from the activation date. The enrollment requires an internet connection and e-mail account. 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. 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.

Murata would like to reiterate that, at this time, there is no evidence that your information was misused. However, Murata encourages you to take full advantage of the services offered.

For More Information

If you have any questions or concerns not addressed in this letter, please call (844) 403-4625 (toll free) Monday through Friday, during the hours of 8:00 a.m. and 5:30 p.m. Central Time (excluding U.S. national holidays). Please have your membership number ready.

Murata sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Yoshi Tanino, President and CEO
For Murata Electronics North America, Inc.

Steps You Can Take to Help Protect Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You have the right to place a security freeze on your credit report with each consumer reporting agency. As of September 21, 2018, it is free to place, lift, or remove a security freeze. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The request must also include full name, Social Security number, complete addresses for the past five years, date of birth, any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles, a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. You may also place a security freeze for children under the age of 16. To place a security freeze on your credit report, you need to make a request to each of the following consumer reporting agencies:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-report-services/credit-freeze/

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. In order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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. You can obtain further information by using the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You have rights under the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable

information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here, including specific additional rights for identity theft victims and active duty military personnel. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For residents of *Oregon*: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of *Arizona*, *Colorado*, *District of Columbia*, *Illinois*, *Maryland*, *New York*, *North Carolina*, and *Rhode Island*: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street**,** Chicago, IL 60601**;** 1-866-999-5630**;** www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division**:** 200 St. Paul Place**,** 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; https://ag.ny.gov/consumer-frauds/identity-theft

North Carolina Office of the Attorney General - Consumer Protection Division**:** 9001 Mail Service Center, Raleigh, NC 27699**;** 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903**;** 1-401-274-4400**;** www.riag.ri.gov

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—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.