April 27, 2026

Company name:	Murata Manufacturing Co., Ltd.
Name of representative:	Norio Nakajima President and Representative Director (Code: 6981, Tokyo Stock Exchange Prime Market)
Contact:	Eiichiro Imazato General Manager of Corporate Communication Department （TEL. +81-75-955-6786）

Notice Regarding Unauthorized Access to Our IT Environment (Update)

Following Murata's previous announcements regarding the unauthorized access to its IT environment by a third party, Murata Manufacturing Co., Ltd. (hereinafter, "Murata") would like to provide an additional update.

1. Background and Overview of the Incident

On February 28, Murata became aware of the possibility of unauthorized access and initiated an initial investigation, and on March 1, a full-scale investigation was commenced. As a result of these investigations, Murata confirmed that unauthorized access had occurred and that data was improperly accessed. Immediately after becoming aware of the potential unauthorized access, Murata established an internal Crisis Response Team and, in cooperation with external cybersecurity experts, has been proceeding with an investigation into the scope of the impact and implementing measures to prevent further damage.

2. Current Situation and Future Actions

Since the previous announcement published on Murata's website on April 6, 2026 (Notice Regarding Unauthorized Access to Our IT Environment (Second Update), Murata has not identified any further damage resulting from the unauthorized access.

Murata's systems are operating normally, and Murata's production and sales activities have not been affected.

Furthermore, Murata has not confirmed that any information that may have been obtained as a result of this incident has been made public on the internet, nor has Murata confirmed any secondary damage or unauthorized use of information resulting from this incident.

With regard to this matter, Murata is coordinating with the necessary relevant authorities and implementing appropriate action under their guidance. Murara is working in cooperation with external cybersecurity experts to strengthen its monitoring of the circulation and publication of information on the internet. Should new information emerge, Murata will carefully assess the details and provide an update promptly.

3.Personal information that may have been leaked as a result of the unauthorized access

The data, including personal information, that has, or might have been, unlawfully obtained by a third party is detailed below (as of April 27).

Potentially affected parties	Data involved	Details
Murata employees and people associated with them (including family members and former employees) Approximately 73,000 cases	Business-related information	Company email address, telephone number, affiliated department, plus information related to HR, employment, and benefits
	Personal information provided to Murata	Full name, date of birth, gender, address, contact details, bank account details, health status, plus other information provided to Murata for various applications and procedures
People outside of Murata (customers, suppliers, and other stakeholders) Approximately 15,000 cases	Information received for the purpose of communication or transactions with Murata	Contact details such as full name, email address, and telephone number, plus other information received in connection to transactions regarding Murata

*The personal information that may have been unlawfully obtained varies for each potentially affected individual, and not all of the information listed in this table was unlawfully obtained for each individual.
* With regard to the number of records for each affected data set, information relating to the same individual may have been counted multiple times.
* There is a risk that non-personal information relating to people outside of Murata, such as invoices, contracts, and sales data from certain business partners, may have been obtained by external parties as a result of the unauthorized access. In order to prevent secondary damage, Murata will refrain from disclosing the details of this information.

4. Measures to prevent recurrence

The measures that Murata has already implemented in light of this incident in order to prevent recurrence are as follows:

・ Blocking access from suspicious sources to the system that was subject to unauthorized access in the recent incident, and enhancing monitoring
・ Strengthening of access restrictions to prevent unauthorized access to the company network
・ Phased implementation of access restrictions to prevent unauthorized access to key cloud environments
・ Strengthening authentication methods and access rights management to prevent unauthorized logins and impersonation attempts
・ Expansion of the scope of security monitoring and detection rules to enable the early detection of cyberattacks and correspondingly rapid responses
・ Strengthening operational processes related to security management to ensure stable security operations

Furthermore, going forward, Murata will implement the following measures as part of Murata's ongoing efforts to enhance security monitoring and continuously improve the security of all its systems, both from a technical and an operational perspective:

・ Continue to thoroughly strengthen authentication methods and access rights management to prevent unauthorized logins and impersonation attempts
・ Continue to enhance detection capabilities and expand the scope of monitoring in preparation for even more sophisticated attacks
・ Strengthen the monitoring of external circulation of company-related information to enable the early

detection of breaches

・ Expand regular external security audits and third-party assessments to establish a continuous cycle of security improvement

5. Impact on Business Performance

The impact of this incident on its business performance is currently under examination. Should new information emerge, Murata will carefully assess the details and provide an update promptly.

Murata sincerely apologizes once again to all stakeholders who may have been affected by this incident.