P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:

https://response.idx.us/KAVX

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

October 30, 2023

NOTICE OF SECURITY INCIDENT

Dear <<FIRST NAME>> <<LAST NAME>>:

Kyocera AVX Components Corporation, and on behalf of its global affiliates and subsidiaries ("KAVX", "we"), writes to inform you of a security incident that has impacted certain types of your personal information as listed below. We are providing you with information about the incident and details related to what you may do to better protect your information, should you feel it necessary to do so.

WHAT HAPPENED? On March 30, 2023, KAVX experienced a cybersecurity incident affecting servers located in Greenville and Myrtle Beach, South Carolina, USA, which resulted in the encryption of a limited number of systems and temporary disruption of certain services. KAVX later discovered that the data contained on the impacted servers included personal information of individuals globally.

Immediately after becoming aware of the incident, KAVX promptly launched a comprehensive investigation with the assistance of third-party cybersecurity experts and notified law enforcement. At the same time, we took proactive measures to remove the unauthorized party and ensure the security of our systems. KAVX's in-depth investigation determined that an unauthorized party gained access to, and took information from, certain systems between February 16, 2023, and March 30, 2023. KAVX also conducted a thorough and time-intensive eDiscovery review of the data contained on the impacted servers in an effort to ensure that we appropriately identify individuals with information potentially impacted, between March and September 2023. After completion of our comprehensive eDiscovery review, KAVX discovered that some of your personal information was impacted.

WHAT INFORMATION WAS INVOLVED? The following types of your personal information have been impacted: <<Variable Data>>.

POSSIBLE CONSEQUENCES OF THE INCIDENT. We are not aware that any of your information has been misused. However, if certain types of your personal information were accessed, then there is a risk that criminals may try to use it to carry out identity theft or fraud. You should always be vigilant of fraud and wary of anyone who asks you for personal information. We understand that you may be concerned by this incident, and we want to help support you.

WHAT WE ARE DOING. Please know that protecting your personal information is something we take very seriously. We conducted a diligent investigation to confirm the nature and scope of the incident. We also took steps to reduce the likelihood of a similar incident occurring in the future, and we continue to make additional improvements that strengthen our cybersecurity protections. Although we have no evidence to suggest your personal information has been fraudulently used, we are nevertheless offering you complimentary CyberScan dark web monitoring, SocialSentry social media monitoring, and Password Detective services for 12 months.

WHAT YOU CAN DO. You can review the enclosed *Recommended Steps to Help Protect Your Information*. You can also enroll to receive the complimentary services being offered to you. Please note the deadline to enroll is January 30, 2024. If your financial information was compromised, we encourage you to remain vigilant by reviewing account statements and reporting anything suspicious to your financial institution. You should also be on guard for schemes where malicious actors may pretend to represent KAVX or reference this incident.

FOR MORE INFORMATION. Please call 1-936-559-2285 or visit https://response.idx.us/KAVX for assistance or for any additional questions you may have. We sincerely regret that this incident occurred.

Sincerely,

Kyocera AVX Components Corporation

Recommended Steps to Help Protect Your Information

1. **Website and Enrollment.** Scan the QR image or go to https://response.idx.us/KAVX and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Telephone. Contact IDX at 1-936-559-2285 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your identity.

3. Review your accounts and credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports (if applicable).

In addition, if your username and password have been compromised, we recommend that you:

Enable two-step authentication on all your online services.

Use strong (long, unusual and complex) passwords and do not use the same password for different online services.

Use a password for your personal email accounts which is different from all your other passwords and ensure it is strong. For example, by using three random words to create your password.

In any case, because of the prevalence of cyber-attacks, we recommend that you take the following precautionary steps:

Be very wary of any phone calls or emails seeking your personal information.

Be alert to emails asking you to click on links, download documents or share your personal details – if you receive an email that seems suspicious, don't open it.