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

Enrollment Code: [redacted]
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 / DATA BREACH>>

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 may have involved your personal information. 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. <<There are [#] Rhode Island residents impacted by this incident.>>

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. On September 19, 2023, after completion of our comprehensive eDiscovery review, KAVX discovered that some of your personal information was potentially impacted. KAVX then initiated an extensive review of its records to confirm the contact details for potentially affected individuals, and on October 1, 2023, we determined your personal information was involved.

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

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 credit monitoring and identity theft protection services for <<12/24>> 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 credit monitoring and identity theft protection services being offered to you.

Please note the deadline to enroll is January 30, 2024. 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 1-888-566-4971 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

IDX
A ZEROFOX COMPANY

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. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-888-566-4971 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

District of Columbia Residents: The District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; +1 (202) 727-3400; oag@dc.gov, and www.oag.dc.gov/.

Iowa Residents: The Attorney General can be contacted at Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319, +1 (515) 281-5164, www.iowaattorneygeneral.gov.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to 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 a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting 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.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.