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

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

RE: Notice of Security Incident

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

Kulicke and Soffa Industries (K&S) writes to inform you about a recent cybersecurity incident that may have involved your personal information. We understand that this can be a stressful situation, and we want to assure you that we are taking this matter very seriously. This letter provides you with information about the nature of the incident and affected data and the immediate and additional corrective measures K&S has taken to guard against future unauthorized disclosure or misuse of your personal data.

What Happened?
On May 12, 2024, K&S discovered its first indications of a ransomware attack when it was contacted by an organization that called itself "LockBit Black." This organization informed K&S that it had accessed and encrypted specific K&S files and showed certain screenshots to support its claims.

K&S subsequently employed a highly reputable third-party forensics team to identify the root cause of the incident and verify the possibility of data access and/or exfiltration. Concurrently, K&S engaged a cyber-negotiator to reach out to the threat actor to provide evidence that could confirm data exfiltration beyond the produced screenshots. On July 12, 2024, the forensics team indicated a possibility that some personal data may have been exfiltrated. This thorough investigation process was conducted (and continues as of the distribution of this letter) to ensure the accuracy and reliability of the information we are providing you. As a result of this ongoing investigation and analysis, we confirmed the identification of your information noted below as of September 16, 2024. However, as of the distribution of this letter, K&S has no reason to believe that your personal information has been used inappropriately or without authorization. This notification was not delayed because of a law enforcement investigation.

What Information Was Involved?
We are notifying you out of an abundance of caution because information related to you was identified in the files that the threat actor potentially accessed. The potentially exposed records included the names, identification numbers, bank account numbers, and/or bank routing numbers of current and/or former employees plus their dependents, and other persons related to K&S.

What We Are Doing
We understand the importance of your personal information and take its security very seriously. Therefore, upon discovering the incident, K&S immediately took comprehensive and proactive steps to protect your data. We reset passwords for all employee accounts, suspended employee mobile email access, identified and removed malicious files, and significantly enhanced our monitoring, logging, and detection capabilities.

We retained global security professionals to conduct an independent investigation and assist with our recovery efforts. After several weeks of investigation, they produced a listing of affected directories, which our professionals and outside counsel then used to harvest and review restored files for potentially affected personal information.

While we do not have any information to suggest that your personal information has been used inappropriately or without

authorization, we have arranged to make available to you 12 months of identity theft resolution services provided by Experian's® IdentityWorks℠ at no charge. Please note that you must enroll to take advantage of this free service, and we encourage you to do so.

What You Can Do
If you have not already done so, you can activate your identity monitoring services by following the instructions in the section below titled *Activating Your Complimentary Identity Monitoring*. As always, please continue to be vigilant about the security of your personal accounts and monitor them for unauthorized activity. Please report any suspicious activity to appropriate law enforcement.

Activating Your Complimentary Identity Monitoring
This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by**: **[Enrollment End Date]** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **[Enrollment URL]**
- Provide your **activation code**: **[Activation Code]**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [Experian TFN] by [Enrollment End Date]. Be prepared to provide engagement number [B######] as proof of eligibility for the Identity Restoration services by Experian.

Additional details regarding your 12-MONTH EXPERIAN IDENTITYWORKS Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- **Credit Monitoring:** Actively monitors Experian, Equifax, and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit-related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level Identity Restoration support even after your Experian IdentityWorks membership expires.
- **Up to $1 Million Identity Theft Insurance[2]:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter, and you can enroll at any time during that period. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection on this site.

For More Information

[1] Offline members will be eligible to call for additional reports quarterly after enrolling.
[2] The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Again, we sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, please contact our call center at [Experian TFN] toll-free Monday through Friday from 8:00 am – 8:00 pm CT (excluding major U.S. holidays). Be prepared to provide your engagement number [B######]. In addition, please review the enclosed attachment called *Preventing Identity Theft and Fraud* for more information about how to protect your personal data. If you would prefer, you may also get in touch with us via email at knsdataenquiry@kns.com.

Sincerely,

Lester Wong
Executive Vice President, Finance and IT and Chief Financial Officer
Kulicke and Soffa Industries, Inc.
1005 Virginia Drive
Fort Washington, PA 19034
1-215-784-6000

Preventing Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Immediately report any suspicious activity to your bank or credit union. If you do find suspicious activity on your credit reports or other statements, call your local police or sheriff's office, or state Attorney General and file a report of identity theft. You have a right to a copy of the police report, and you may need to give copies of the police report to creditors to clear up your records and access some services free to identity theft victims.

Under the U.S. Fair Credit Reporting Act and other laws, you have certain rights that can help protect yourself from identity theft. Many of these are explained in this letter and at www.identitytheft.gov/#/Know-Your-Rights. For example, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

In addition, at no charge, you can have these credit bureaus place a short-term or an extended "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because a fraud alert tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. Once one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. If you wish to place a fraud alert or have any questions regarding your credit report, please contact any one of the agencies listed below. Please note: no one except you is allowed to place a fraud alert on your credit report.

General contact information for each agency:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19016-2000
1-866-349-5191	888-397-3742	800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

To add a fraud alert:

Equifax	(888) 202-4025, Option 6 or	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
Experian	(714) 830-7000, Option 2 or	https://www.experian.com/fraud/center.html
TransUnion	(800) 916-8800, Option 0 or	https://www.transunion.com/fraud-alerts

You may also place a security freeze on your credit reports, free of charge. A security freeze, also known as a "credit freeze," prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. Unlike a fraud alert, you must place a security freeze separately on your credit file at each bureau. You can use the following addresses and contact information to place a security freeze with each major credit bureau:

Equifax Security Freeze. 1-888-298-0045. P.O. Box 1057881, Atlanta, GA 30348-0241. www.equifax.com/personal/credit-report-services/credit-freeze;

Experian Security Freeze. 1-888-EXPERIAN or 1-888-397-3742. P.O. Box 9554, Allen, TX 75013. www.experian.com/freeze/center.html; or

TransUnion. 1-800-680-7289. Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19016-2000. www.transunion.com/credit-freeze

The Federal Trade Commission also provides additional information about credit freezes here: https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

In order to request a security freeze, you may need to supply your full name (including middle initial, as well as Jr., Sr., II, III, etc.), date of birth, Social Security number, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or another statement to show proof of your current address. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning your identity theft.

The credit reporting agencies must place a security freeze on your credit report within one (1) business day after receiving a request by phone or secure electronic means and within (3) business days after receiving your request by mail. The credit bureaus must then send

written confirmation to you within five (5) business days of placing the security freeze, along with information about how to remove or lift the security freeze in the future.

You can further educate yourself regarding identity theft, fraud alerts, freezes, and the steps you can take to protect yourself by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission encourages those who discover their information has been misused to file a complaint with them. Instances of known or suspected identity theft should also be reported to law enforcement or your state Attorney General.

The Federal Trade Commission can be reached at:

Federal Trade Commission
Consumer Resource Center
600 Pennsylvania Avenue NW Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.identitytheft.gov **or** www.ftc.gov

OTHER IMPORTANT INFORMATION
You may file a report with your local police or the police in the community where the identity theft occurred. You are entitled to request a copy of your police report filed in that matter.

California residents:
You can visit the California Attorney General's site (www.oag.ca.gov/idtheft) for additional information on protection against identity theft.

Iowa residents:
You are advised to report any suspected identity theft to law enforcement or the Iowa Attorney General.

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

Maryland residents:
You may obtain information about avoiding identity theft at: Office of the State of Maryland Attorney General, 200 St. Paul Place Baltimore, MD 21202; phone: 1-888-743-0023; www.marylandattorneygeneral.gov.

New Mexico residents:
The Fair Credit Reporting Act (FCRA) provides certain rights in addition to the right to receive a copy of your credit report (including a free copy once every 12 months), including the right to ask for a credit score, dispute incomplete or inaccurate information, limit "prescreened" offers of credit and insurance, be told if information in your credit file has been used against you, and seek damages from violators. You may have additional rights under the FCRA not summarized here, and identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. You can review these rights by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

North Carolina residents:
You may obtain information about avoiding identity theft at: North Carolina Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001; phone: 919-716-6400; ncdoj.gov

Oregon residents:
You may obtain information about avoiding identity theft at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; phone: 1-877-877-9392; www.doj.state.or.us/.

Rhode Island residents:
You may obtain information about preventing and avoiding identity theft from Rhode Island's Attorney General Office: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903; phone: 401-274-4400; http://www.riag.ri.gov.

Washington D.C. residents:
You may obtain information about avoiding identity theft at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001; phone: 202-727-3400; https://oag.dc.gov/.

Colorado, Georgia, Maine, Maryland, Massachusetts, and New Jersey residents:
You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).