



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Katie Butler
Office: (267) 930-1613
Fax: (267) 930-4771
Email: kbutler@mullen.law

609 SW 8th Street., Suite 600
Bentonville, AR 72712

January 24, 2022

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Ensinger Industries Inc. (“Ensinger”) located at 365 Meadowlands Boulevard, Washington, PA 15301, and are writing to notify your office of an incident that may affect the security of some personal information relating to eight (8) Maryland residents. By providing this notice, Ensinger does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On July 2, 2021 Ensinger discovered a cyber event impacting its internal systems. In response, it immediately began an investigation with the assistance of third-party forensic investigators to determine the nature and scope of the activity. The investigation confirmed that the Ensinger network was subject to unauthorized access between June 13, 2021 and July 2, 2021. In response, Ensinger worked diligently to determine the nature of information that may have been impacted, and to whom that information pertained.

The information that could have been subject to unauthorized access includes name and Social Security Number.

Notice to Maryland Residents

On or about January 24, 2022, Ensinger provided written notice of this incident to all affected individuals, which includes eight (8) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the incident, Ensinger moved quickly to investigate and respond, assess the security of Ensinger systems, and notify potentially affected individuals. Ensinger is also working to implement additional safeguards and training to its employees. Ensinger reported the incident to law enforcement and will cooperate with any investigation. Ensinger is providing access to credit monitoring and identity theft protection services for 24 months, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Ensinger is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Ensinger is providing individuals with 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1613.

Very truly yours,

Katie Butler of
MULLEN COUGHLIN LLC

KLB/ara
Enclosure

EXHIBIT A



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

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

<<b2b_text_1(header - NOTICE OF SECURITY INCIDENT / NOTICE OF DATA BREACH)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Ensinger Industries, Inc. ("Ensinger") is writing to notify you of a recent incident that may have impacted the security of your information. We want to provide you with information about the incident, our response, and steps you may take to better protect against possible misuse of your personal information, should you feel it necessary to do so.

What Happened?

On July 2, 2021 Ensinger discovered a cyber incident impacting our internal systems. In response, we immediately began an investigation with the assistance of third-party computer forensic specialists to determine the nature and scope of the incident. The investigation confirmed that the Ensinger network was subject to unauthorized access between June 13, 2021 and July 2, 2021. We therefore undertook a meticulous review of the potentially impacted files and our internal systems to identify the information that was involved and to whom it related. Unfortunately, on October 19, 2021, we determined that some information relating to you may have been subject to unauthorized access. We then worked to determine mailing addresses for those impacted by the event. Although we are unaware of any actual or attempted misuse of your information, we are providing you this notification in an abundance of caution.

What Information Was Involved?

The impacted information relating to you includes your name and Social Security Number.

What We Are Doing.

Information security is among our highest priorities, and we are continually reassessing our security measures to protect information in our care. Upon discovering the incident, we secured the network and investigated to determine those individuals that were affected. We have taken additional steps to improve security and better protect against similar incidents in the future. We also reported the incident to law enforcement. We have and will continue to cooperate with any subsequent inquiries and investigation. We are also notifying potentially affected individuals, including you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so. Although we are unaware of any actual or attempted misuse of your personal information as a result of this incident, we arranged to have Kroll provide credit and identity monitoring plus restoration services for 24 months at no cost to you as an added precaution.

What You Can Do.

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next 24 months. Information on how to activate your free credit and identity monitoring is included in the attached Steps You Can Take to Help Protect Personal Information. Please review this attachment for more information on steps you can take to further protect yourself.

For More Information.

We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call (855) 618-3208, 8:00 am to 5:30 pm Central Time, excluding major U.S. holidays. Please have your membership number ready.

Sincerely,

A handwritten signature in black ink that reads "Bill". The signature is stylized with a long, sweeping horizontal stroke above the letters.

William R. Matthews III
Vice President – Administration

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Activate Credit and Identity Monitoring and Restoration

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide credit and identity monitoring and restoration at no cost to you for 24 months. Kroll is a global leader in risk mitigation and response, and its team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. If you are currently enrolled in Identity Monitoring and Restoration through Kroll, please contact the call center at (855) 618-3208 to take advantage of this offer, rather than signing up online as described below.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

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

Single Bureau Credit Monitoring

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. 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.

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.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;

3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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 on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Ensinger Industries, Inc. is located at 365 Meadowlands Blvd., Washington, PA 15301.

For 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 bureaus 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 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. We encourage you to 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.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed regarding this incident. There are [#] Rhode Island residents impacted by this incident.