# EXHIBIT 1

By providing this notice, Ensinger Industries, Inc. does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

## Nature of the Data Event

On or about February 17, 2021 Ensinger Industries, Inc. discovered employees at four (4) US locations (PA, NJ, DE, CA) and certain remote employees were unable to access company network and or systems and several received a message that their account was hacked, they should not move or rename encrypted files, and should not shut down or restart their machines. In response, Ensinger Industries, Inc. worked with outside specialists to investigate the nature and scope of the event. Ensinger Industries, Inc. determined that parts of their network were subject to unauthorized access between February 8, 2021 and February 17, 2021. Ensinger Industries, Inc. reviewed the parts of their network determined to be subject to unauthorized access and determined that personal information relating to four (4) Indiana residents may have been impacted. The types of information impacted relating to Indiana residents are their names, Social Security number and date of birth.

## Notice to Maine Resident

On or about May 7, 2021, Ensinger Industries, Inc. provided written notice of this incident to all affected individuals, which includes one (1) Maine resident. 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 event, Ensinger Industries, Inc. moved quickly to investigate and respond to the incident, assess the security of Ensinger Industries, Inc. systems, and notify potentially affected individuals. Ensinger Industries, Inc. is also working to implement additional safeguards and training to its employees. Ensinger Industries, Inc. is providing access to credit monitoring 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 Industries, Inc. 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 Industries, Inc. is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

# EXHIBIT A

Ensinger

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

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

**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 Wednesday morning, February 17, 2021 several data centers supporting the Ensinger US Group businesses were the victim of a cyber-attack, rendering various systems inoperable and locking much of our information. In response, Ensinger immediately worked with third party forensic investigators to investigate the nature and scope of the activity, and conducted a deliberate, thorough, and comprehensive assessment of our network. Our investigation determined that an unknown individual accessed or acquired data contained within certain segments of our network between February 8, 2021 and February 17, 2021. On April 16, 2021 we confirmed that information relating to you was impacted by this event. Although information relating to you may have been accessible, there is no indication that this information was actually viewed by an unauthorized actor. However, we are notifying you of this incident in an abundance of caution.

**What Information Was Involved?** The investigation determined that your <<b2b_text_1(DataElements)>> may have been accessible to an unauthorized actor.

**What We Are Doing**. The confidentiality, privacy, and security of personal information within our care is among Ensinger's highest priorities. Upon learning of the event, we investigated to determine those individuals that were affected, and secured the network. We have taken additional steps to improve security and better protect against similar incidents in the future. 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 event, we arranged to have Kroll protect your identity 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 12 to 24 months. You may also review the information contained in the attached *Steps You Can Take to Help Protect Your Information.* There you will also find more information on the identity monitoring services we are making available to you.

**For More Information.** If you have questions, please call 1-855-498-2048, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready. Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Bill

William R. Matthews III
Executive Vice President – Administration

## Steps You Can Take to Protect Personal Information

### Activate Identity Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **July 13, 2021** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

### 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 |
| 1-888-298-0045 | 1-888-397-3742 | 1-833-395-6938 |
| 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.