

## NOTICE OF DATA INCIDENT

### ABOUT THE DATA PRIVACY EVENT

Consolidated Electrical Distributors (“CED”) is providing notice of an incident that may affect the privacy of certain information so that potentially affected individuals and businesses may take steps to better protect their information, should they feel it appropriate to do so.

### FREQUENTLY ASKED QUESTIONS

***What Happened?*** Consolidated Electrical Distributors, Inc. (“CED”) became aware of unusual activity in an employee’s email account and launched an investigation with the assistance of a third-party forensic investigator to determine the full nature and scope of what occurred. Through this investigation, CED determined that certain employees fell victim to an email phishing scam that led to their credentials being compromised and an unknown actor gained access to their email accounts between August 11, 2019 and November 11, 2019. The email credentials were changed, and the email accounts are now secure.

The content of the accounts was reviewed through a time-consuming manual and programmatic process to determine what sensitive data may have been accessible. CED confirmed the types of protected information contained in the affected email accounts and the locations of the individuals and businesses to which the information relates. Although CED is unaware of any actual or attempted misuse of any information, CED is providing notification of this incident out of an abundance of caution.

***What Information Was Involved?*** While, to date, the investigation has found no evidence of actual or attempted misuse of data, CED did determine that the email accounts affected by this incident may include name, payment card information, Social Security number, financial account information, passport number, driver’s license or other government issued ID number, treatment information, patient account number, medical record number, and/or username and password.

***What is CED Doing?*** Upon learning of this incident, CED reset account passwords and quickly took steps to determine the content of the impacted accounts and identify the potentially impacted individuals and entities. CED will also notify the necessary regulatory bodies. In an abundance of caution, CED is notifying potentially impacted individuals and entities. Additionally, while CED has safeguards in place to protect data in its care, it is working to review and enhance these protections as part of its ongoing commitment to data privacy and security.

On July 14, 2020, CED began mailing notice letters to individuals and businesses whose information may have been present in the affected email accounts. CED offered the affected individuals access to credit monitoring and identity restoration services for one year without charge.

***What You Can Do.*** CED encourages individuals and businesses to review and consider the information and resources outlined in the below “Steps You May Take to Protect Personal Information.”

***For More Information.*** You may write to CED at 1920 Westridge Drive, Irving, TX 75038 or call 1-844-951-2882 Monday through Friday, between 8:00 a.m. and 5:30 p.m. CT (excluding U.S. holidays), with any additional questions.

## STEPS YOU MAY TAKE TO PROTECT PERSONAL INFORMATION

### Monitor Your Accounts

CED encourages potentially impacted individuals to remain vigilant against incidents of identity theft and fraud by reviewing their accounts, explanations of benefits, and credit reports for suspicious activity, to detect errors. You are encouraged to report any suspicious activity to the affiliated institutions immediately. Under U.S. law, individuals with credit reports 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](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

#### **Experian**

PO Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

#### **TransUnion**

P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

#### **Equifax**

PO Box 105788  
Atlanta, GA 30348-5788  
1-800-349-9960

[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your 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 agencies listed below:

**Experian**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

**TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289

[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

**Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-800-525-6285

[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338); 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 North Carolina residents, the Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, [www.ncdoj.gov](http://www.ncdoj.gov). You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.