EXHIBIT 1

This notice will be supplemented with any significant facts learned subsequent to its submission. By providing this notice, CED 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 November 10, 2020, CED became aware of unusual activity in an employee email account. CED launched an investigation 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 on November 10, 2020. The email credentials were changed, and the email accounts are now secure.

The content of the accounts was then reviewed through a manual and programmatic process to determine what sensitive data may have been accessible. CED then confirmed the identities of the individuals who may have had information accessible as a result of the incident, and launched a review of internal files to ascertain address information for the impacted individuals. Although CED is unaware of any actual or attempted misuse of any information, notification is being provided to potentially impacted individuals out of an abundance of caution.

The information that could have been subject to unauthorized access includes name, address, Social Security number, financial account information, driver's license or other government issued identification number, username and password, PIN, and or account login.

Notice to Maine Residents

On or about April 12, 2021, CED provided written notice of this incident to potentially affected individuals, which includes ninety six (96) Maine 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 event, CED moved quickly to investigate and respond to the incident, assess the security of CED systems, and notify potentially affected individuals. CED is also working to implement additional safeguards and training to its employees. CED is providing access to credit monitoring services for one year through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, CED 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. CED 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.

EXHIBIT A

CONSOLIDATED ELECTRICAL DISTRIBUTORS, INC.

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

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

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

Consolidated Electrical Distributors ("CED"), including DBAs under which it operates, is writing to notify you of an incident that may affect the security of some of your information. This letter provides details of the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened. On November 10, 2020 CED became aware of unusual activity in an employee email account. We launched an investigation 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 on November 10, 2020. The email credentials were changed, and the email accounts are now secure.

The content of the accounts was reviewed through a manual and programmatic process to determine what sensitive data may have been accessible. We then confirmed the identities of the individuals who may have had information accessible as a result of the incident, and launched a review of our files to ascertain address information for the impacted individuals. Although we are unaware of any actual or attempted misuse of your information, we are providing you this notification out of an abundance of caution because your information was present in the impacted email accounts.

What Information Was Involved. The investigation confirmed that the following types of information may have been accessible as a result of the incident: <<b2b_text_1(DataElements)>>. We have no evidence this information has been subject to actual or attempted misuse.

What We Are Doing. Upon learning of this incident, we reset account passwords and quickly took steps to determine the content of the impacted account and identify the potentially impacted individuals. We will also notify the necessary regulatory bodies. In an abundance of caution, we are notifying potentially impacted individuals, including you, so that you may take further steps to best protect your information, should you feel it is appropriate to do so. Although we are unaware of any actual or attempted misuse of your information as a result of this incident, we are offering identity monitoring services through Kroll for twelve (12) months at no cost to you as an added precaution. Additionally, while we have safeguards in place to protect data in our care, we are working to review and enhance these protections as part of ongoing commitment to data privacy and security.

What You Can Do. You may review the information contained in the attached "Steps You Can Take to Protect Personal Information." You may also activate the identity theft protection services we are making available to you through Kroll. CED will cover the cost of this service for twelve (12) months; however, you will need to activate yourself in this service.

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-855-723-1669 (toll free), Monday – Friday, 8:00 a.m. to 5:30 p.m., Central Time.

We sincerely regret any inconvenience this incident may cause you. CED remains committed to safeguarding information in our care.

Sincerely,

Consolidated Electrical Distributors, Inc.

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, 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 8, 2021** to activate your identity monitoring services.*

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

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, military identification, 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 fraud alert or 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.

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. Consolidated Electrical Distributors, Inc. is located at 1920 Westridge Drive, Irving, TX 75038.

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.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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 will 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.