NORTON ROSE FULBRIGHT

March 25, 2022

Sent by Certified Mail

Office of the New Hampshire Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Norton Rose Fulbright Canada LLP
400 3rd Avenue SW, Suite 3700
Calgary, Alberta T2P 4H2 Canada

F: +1 403.264.5973
nortonrosefulbright.com

John Cassell
+1 403.267.8233
john.cassell@nortonrosefulbright.com

Assistant
+1 403.267.8341
erika.canning@nortonrosefulbright.com

Dear Madam or Sir:

Notice of Information Security Incident

I am writing on behalf of my client, Cooledge Lighting Inc. ("Cooledge"), to provide notice of a security incident that involved four (4) New Hampshire residents.[1]

On March 6, 2022, Cooledge discovered suspicious activity within its network. In response, it immediately took action to secure the network and launched an investigation with the assistance of cybersecurity and forensic specialists. Cooledge also notified law enforcement on March 22, 2022.

The investigation determined that an unauthorized third party accessed certain information pertaining to some of our current and former employees. The data accessed by the unauthorized third party included names, dates of birth, Social Security numbers, and other employment-related information. Cooledge is not aware of any identity theft, fraud, or misuse of the employees' information stemming from this incident.

Beginning March 25, 2022, Cooledge is notifying the affected New Hampshire residents via US mail. Enclosed is a sample copy of the letter being mailed to the four New Hampshire residents. Cooledge is offering 24 months of complimentary credit monitoring and identity protection services through CyberScout as well as a toll free hotline for the individuals to call with any questions they may have.

[1] This notice does not waive Cooledge's objection that New Hampshire lacks personal jurisdiction over it regarding any claims related to this data security incident.

NORTON ROSE FULBRIGHT

Since the incident, Cooledge has taken significant steps and will continue to look for means to enhance its security procedures.

Yours very truly,

Norton Rose Fulbright Canada LLP

John Cassell
Partner

JC/kd

COOLEDGE™

cooledgelighting.com

110–13551 Commerce Parkway
Richmond, BC V6V 2L1
Canada

O +1 604 273 2665
F +1 604 273 2660

March 25, 2022

Dear [redacted]

RE: Notice of Data Breach

At Cooledge Lighting Inc., we take the privacy and security of our current and former employees' information seriously. We are writing to inform you of a cybersecurity incident that involved some of your information. This letter explains the incident, steps we are taking to bolster the protection of your information in our systems, and steps you can take in response.

What Happened?

On March 6, 2022, we discovered that an unauthorized individual had gained access to some Cooledge systems. We immediately initiated an investigation with the assistance of cybersecurity and forensic specialists and took steps to enhance the security of our network. We also notified law enforcement. Our investigation determined that the unauthorized third party accessed certain information pertaining to some of our current and former employees. While we have no knowledge of any misuse of any personal information as a result of this incident, we wanted you to be aware and to know that we take it seriously.

What Information Was Involved?

As an employer, Cooledge collects a range of general contact and profile information. Our investigation determined that the following types of your information was involved: your name, date of birth, Social Security number, hire date, termination date and compensation. Again, at this time, we have no reason to believe that your personal information has been misused.

Please note that not all of the above information has been compromised for each individual.

What We Are Doing

Upon discovery of this incident, Cooledge immediately engaged a team of cybersecurity experts to contain the incident and conduct a thorough investigation to determine how the incident occurred, the extent of the compromise, and to assist Cooledge in its remediation efforts.

In an effort to provide assistance to former and current employees, Cooledge is offering you 24 months of complimentary identity theft and credit monitoring services through CyberScout. With

COOLEDGE

these services, you will be able to receive regular alerts to inform you of any important changes to your credit file.

Your unique activation code to register for CyberScout's services is [redacted]

To activate your account, please visit https://www.myidmanager.com and enter your unique activation code by July 31, 2022.

To prevent fraudulent access to your credit file, you will be subject to a verification and authentication process. You will be required to provide certain personal information such as your date of birth, address and telephone number in order to be successfully authenticated.

What You Can Do

While there is no evidence that any of your personal information was misused as a result of this incident, we encourage you to always remain vigilant against identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. As explained above, we are also providing you complimentary credit monitoring and identity theft protection services. For additional information on steps you can take to protect your identity, please review the information included with this letter.

For More Information

If you have any questions in relation to the incident, please contact Louise Van at louise.van@cooledgelighting.com.

Sincerely,

Louise Van
Vice President, Human Resources

COOLEDGE

ADDITIONAL STEPS YOU CAN TAKE

Free Credit Report. Regardless of whether you choose to take advantage of the complimentary identity monitoring, it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Contact information for the three nationwide credit reporting companies is as follows:

Equifax	**Experian**	**TransUnion**
Phone: 1-800-685-1111	Phone: 1-888-397-3742	Phone: 1-800-888-4213
P.O. Box 105788	P.O. Box 2390	P.O. Box 1000
Atlanta, Georgia 30348	Allen, Texas 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

Don't confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

COOLEDGE

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. You may obtain information from the credit reporting agencies and the FTC about security freezes.

Upon receiving a request for a security freeze, each credit bureau will provide you with a unique identification number or password. Keep the number or password secure, as you will need it if you choose to lift the freeze. If you request a freeze be lifted (either temporarily or entirely), a credit bureau must lift the freeze within one hour if it is requested online or via phone. If requested by mail, a credit bureau must lift the freeze no later than three business days after receipt.

Fraud Alerts. You may ask that a fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut Residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

COOLEDGE

For New York Residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697- 1220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov. You may also contact Cooledge Lighting Inc. at 110-13551 Commerce Parkway, Richmond, British Columbia V6V 3B9 or 604-273-2665.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may contact the Massachusetts Office of the Attorney General, 1 Ashburn Place, 20th Floor, Boston, MA 02108, www.ago.state.ma.us, 1-617-727-8400.

Reporting of identity theft and obtaining a police report.

You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

If you know or suspect you are a victim of tax-related identity theft, the IRS recommends these steps:

Respond immediately to any IRS notice; call the number provided or, if instructed, go to IDVerify.irs.gov.

Complete IRS Form 14039, Identity Theft Affidavit, if your e-filed return rejects because of a duplicate filing under your Social Security number or you are instructed to do so. Use a fillable form at IRS.gov, print, then attach the form to your return and mail according to instructions.

Continue to pay your taxes and file your tax return, even if you must do so by paper.

If you previously contacted the IRS and did not have a resolution, contact the IRS for specialized assistance at 1-800-908-4490.

COOLEDGE

Activation Code: l152jw0v0b8g

We have retained the assistance of Cyberscout, a company specializing in fraud assistance and remediation services.

Through Cyberscout, we have arranged a two-year subscription to Credit Monitoring services*, at no cost to you. Cyberscout has been retained to help you with any questions or problems you may encounter, including assisting you with obtaining a credit report and placing fraud alerts.

We encourage you to take advantage of this service and help protect your identity. To activate your service, please visit:

https://www.myidmanager.com

You will be prompted to enter the following activation code:

[redacted]

Please ensure that you redeem your activation code before 7/31/2022 to take advantage of the service.

Upon your completion of the enrollment process, you will have access to the following features:

- Access to a credit report with credit score. A credit report is a snapshot of a consumer's financial history and primary tool leveraged for determining credit-related identity theft or fraud.
- Credit monitoring alerts with email notifications to key changes on a consumer's credit file. In today's virtual world, credit alerts are a powerful tool to protect against identity theft, enable quick action against potentially fraudulent activity, and provide overall confidence to potentially impacted consumers.
- Dark Web Monitoring to provide monitoring of surface, social, deep, and dark websites for potentially exposed personal, identity and financial information in order to help protect consumers against identity theft.
- Identity theft insurance of up to $1,000,000 in coverage to protect against potential damages related to identity theft and fraud
- Assistance with reading and interpreting credit reports for any possible fraud indicators.
- Assistance with answering any questions individuals may have about fraud.

Should you have any questions regarding the Cyberscout solution, have difficulty enrolling, or require additional support, please contact Cyberscout at 1-800-405-6108 from Monday to Friday 8:00 am – 8:00 pm EST, excluding holidays.

COOLEDGE

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.