

20438

From: From_The_Desk_of_Matt_Roney <fromthedeskofmattroney@lumileds.com>
Sent: Monday, May 10, 2021 1:02 PM
To: [REDACTED]
Subject: Lumileds – Notice of Data Breach



Lumileds
370 W. Trimble Road
San Jose, CA 95131

May 10, 2021



Lumileds – Notice of Data Breach

Dear Lumileds Former Colleague or Consultant,

This email is to inform you about a cybersecurity incident involving data maintained by Lumileds.

What Information Was Involved?

Some of your personal data was among the data affected by the cybersecurity incident and/or may have been removed by the unauthorized third party. This may have included your name and surname, contact information, date of birth, gender, compensation details, hire date, job title and grade, offer letter, pension information, passport number, national ID number, nationality, social security number, banking account number, mortgage statement, place of birth, marital status, spouse and children's names and surnames, spouse and children's dates of birth, performance reviews, and termination details.

What Are We Doing?

At this time, we have no proof that your data has been misused. Nevertheless, we have reported this incident to law enforcement authorities and are assisting their investigation. Lumileds is also complying with its data privacy regulatory obligations.

We take this matter extremely seriously. We have engaged outside cybersecurity experts to assist us in understanding the incident; have increased our security monitoring including by rolling out new tools in our network; and are actively reviewing the incident to identify further measures that can be taken to enhance our cybersecurity posture.

What You Can Do

As noted above, we have no proof that your data has been misused. You should remain vigilant for any unusual communications that may be created based upon the data that was exposed, such as targeted "phishing" emails. You should also monitor your financial accounts for any unexplained activity, and your mail for any evidence of unfamiliar accounts as these could be signs of fraud.

To help protect you, we have secured the services of Equifax to provide you with two years of credit and identity monitoring in the U.S. and Canada, or one year of identity monitoring, where these services are available in your country, at no cost to you.^[1] To find out whether these services are available in your country and to enroll in these services, please contact us at Creditmonitoring@Lumileds.com.

For More Information

Please contact Privacy@Lumileds.com if you have other general data questions. Lumileds can be contacted at: 370 W. Trimble Road, San Jose, CA 95131 or by phone at 408-964-2900.

We thank you again for your patience while we address this matter.

Matt Roney
CEO

Additional Resources for Residents of the United States

You should remain vigilant for instances of fraud or identity theft by reviewing your account statements and closely monitoring your credit reports, which are available to you free of charge. You may obtain a free copy of your credit report once every 12 months from each of the three nationwide credit reporting agencies. Contact information for these agencies is as follows:

Equifax: P.O. Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-525-6285

Experian: P.O. Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion: P.O. Box 2000, Chester, PA 19022, www.transunion.com, 1-800-680-7289

Annual Credit Report. You may also order a free annual credit report. To do so, please visit www.annualcreditreport.com or call 1-887-322-8228.

You can also order your free annual 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/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alert. You may place a fraud alert in your file by contacting one of the three nationwide credit reporting agencies listed above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a security freeze on your credit report. A security freeze will prevent new credit from being opened in your name without the use of a PIN number that will be issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the credit reporting agency certain identifying information, including your full name; Social Security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or insurance statement. There is no fee to place or lift a security freeze.

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 can 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/IDTHEFT, 1-877-IDTHEFT (438-4338).

Federal Fair Credit Reporting Act Rights: The Fair Credit Reporting Act ("FCRA") is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies 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 reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; you may seek damages from violators. Identify theft victims and active duty military personnel have additional rights. For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Police Report: Under Massachusetts law, you have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file

^[1] These services are unavailable in China or France, among other countries.