



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Angelina W. Freind
Office: (267) 930-4782
Fax: (267) 930-4771
Email: afreind@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

March 19, 2021

VIA U.S. MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent LI-COR, Inc. ("LI-COR") located at 4647 Superior Street, Lincoln, NE 68504-5000 and are writing to notify your office of an incident that may affect the security of some personal information relating to nine (9) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, LI-COR does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On February 16, 2021, LI-COR experienced a service disruption that was determined to be caused by a sophisticated cyber-attack. LI-COR immediately launched an investigation to determine the nature and scope of this incident, working with outside cybersecurity specialists to securely restore the impacted systems. LI-COR also notified federal law enforcement and is cooperating, as required.

The investigation identified a limited number of files and folders within the LI-COR environment that were accessed and/or acquired by the unknown actor. On or about March 5, 2021, LI-COR confirmed that personal information for certain individuals was present in the files and folders that may have been accessed, and worked as quickly as possible to identify and notify these individuals. The information that could have been subject to unauthorized access includes name, Social Security number, and financial account information.

Mullen.law

STATE OF NH
DEPT OF JUSTICE
2021 MAR 24 PM 2:48

Notice to New Hampshire Residents

On March 19, 2021 LI-COR provided written notice of this incident to affected individuals, which includes approximately nine (9) New Hampshire 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

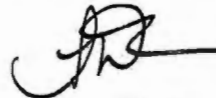
Upon discovering the event, LI-COR moved quickly to investigate and respond to the incident, assess the security of LI-COR systems, and notify potentially affected individuals. LI-COR is also working to implement additional safeguards. LI-COR is providing access to credit monitoring services for 12 months through Cyberscout to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, LI-COR 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. LI-COR 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4782.

Very truly yours,



Angelina W. Freind of
MULLEN COUGHLIN LLC

AWF/kjc
Enclosure

EXHIBIT A

IMS c/o LI-COR, Inc.
245 Commerce Blvd
Liverpool NY 13088



March 19, 2021

Re: Notice of Data Breach

Dear _____ :

LI-COR, Inc. ("LI-COR") writes to inform you of an incident that may affect the security of some of your personal information. This notice provides information about the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? On February 16, 2021, LI-COR experienced a service disruption that was determined to be caused by a sophisticated cyber-attack. We immediately launched an investigation to determine the nature and scope of this incident, working with outside cybersecurity specialists to securely restore our systems. The investigation identified a limited number of files and folders within the LI-COR environment that were accessed and/or acquired by the unknown actor. On or about March 5, 2021, we confirmed that personal information for certain individuals was present in the files and folders that may have been accessed and worked as quickly as possible to identify and notify these individuals

What Information Was Involved? The investigation determined that the following types of your personal information were present in the files and folders accessed and/or acquired by the unknown actor at the time of the incident:

What We Are Doing. We take this incident and the security of personal information in our care seriously. Upon learning of this incident, we moved quickly to investigate and respond to this incident, assess the security of relevant systems, and notify potentially affected individuals. Our response included resetting relevant account passwords, reviewing the contents of the potentially accessed files and folders to determine whether they contained protected information, and reviewing internal systems to identify contact information for purposes of providing notice to potentially affected individuals. We also notified and are cooperating with Federal law enforcement. As part of our ongoing commitment to the security of information, we are also reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event.

LI-COR notified law enforcement of this incident and is notifying relevant state and federal regulators. We are also offering you access to complimentary credit monitoring and identity protection services for 12 months through CyberScout. These services include fraud consultation and identity theft restoration services. If you wish to activate the credit monitoring and identity protection services, you may follow the instructions included in the *Steps You Can Take to Help Protect Personal Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and credit reports for suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Help Protect Personal Information*. There you will also find more information on the credit monitoring and identity protection services we are making available to you. While LI-COR will cover the cost of these services, you will need to complete the activation process.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call Cyberscout's call center at 1-800-405-6108 from 8:00 am to 5:00 pm Eastern time, Monday through Friday for 90 days from the date of this letter. You may also write to LI-COR at: 4647 Superior Street, Lincoln, NE 68504-5000.

We sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,



Gregory L. Biggs
CEO & President
LI-COR, Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

Cyberscout representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 5:00 pm Eastern time, Monday through Friday. Please call the Cyberscout help line 1-800-405-6108 and supply the fraud specialist with your access code listed below. To extend these services, enrollment in the monitoring services described below is required.

Additionally, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score/Cyber Monitoring* services at no charge as well as access to a Fraud Specialist and remediation support in the event you become a victim of fraud. These services will be available to you at no charge for twelve (12) months and will begin as soon as you complete your registration. When changes occur to your Experian credit file, notification is sent to you the same day the change or update takes place with the bureau. Cyber Monitoring scans the dark web and alerts you if your personally identifiable information is found. To safeguard your privacy and security, you will be asked to verify your identity before monitoring can be activated.

How do I enroll for the free services?

To Register your account and activate your services:

1. Type the following URL into your browser: <https://www.cs4protect.com> or **cs4protect.com**
2. Click the "Sign Up" button and follow the instructions to create your account.

Enter your information and the following Access Code to complete your registration:

3. Next, click the "Use Now" link on the Monitoring Services tile to verify your identity and activate your monitoring services.

Important – you must register your account and activate your monitoring services within 90 days from the date of this letter, otherwise your ability to access the services will expire.

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
888-298-0045	1-888-397-3742	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. LI-COR is located at 4647 Superior Street, Lincoln, NE 68504-5000.

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.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.