



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Lynda Jensen
Office: (267) 930-2303
Fax: (267) 930-4771
Email: Ljensen@mullen.law

3 Allied Drive, Suite 303
Dedham, MA 02026

October 12, 2022

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Lindberg & Ripple (“Lindberg”) located at 29 South Main St., Suite 311, West Hartford, CT 06107, and are writing to notify your office of an event that may affect the security of certain personal information relating to eleven (11) Maryland residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Lindberg does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland event notification statute, or personal jurisdiction.

Nature of the Data Event

On or around December 14, 2021, Lindberg identified suspicious activity related to an employee’s email account. Upon learning of the suspicious activity, Lindberg immediately took steps to secure the email account and launched an investigation to determine the nature and scope of the event. The investigation confirmed that an unknown actor had access to two email accounts, one between November 24, 2021 and December 14, 2021 and another for a limited time period prior to April 18, 2021. The investigation could not determine what emails, if any, the unknown actor accessed. In an abundance of caution, Lindberg worked with specialists to perform a comprehensive programmatic and manual review of the information stored in the email accounts at the time of event to identify the types of information contained within the accounts and to whom the information related. On April 29, 2022, this extensive review identified certain customer and/or employee information was present within the records. Lindberg then conducted a thorough review of their records to confirm the identities and contact information for potentially affected individuals. This review was completed on or about September 23, 2022.

The information that could have been subject to unauthorized access includes name, Social Security number, driver's license number and medical information.

Notice to Maryland Residents

On October 12, 2022, Lindberg provided written notice of this event to eleven (11) Maryland 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, Lindberg moved quickly to investigate and respond to the event, assess the security of Lindberg systems, and identify potentially affected individuals. Lindberg is providing access to credit monitoring services for one year (1) year, through IDX, to individuals whose personal information was potentially affected by this event, at no cost to these individuals.

Additionally, Lindberg is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Lindberg is providing individuals with information on how to place a fraud alert and a credit freeze on their credit files, 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 Attorneys General, and law enforcement to report attempted or actual identity theft and fraud. Lindberg is providing written notice of this event to relevant state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-2303.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Lynda Jensen".

Lynda Jensen of
MULLEN COUGHLIN LLC

LRJ/nad
Enclosure

EXHIBIT A

Lindberg & Ripple
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223



Lindberg & Ripple
Deeper Insights. Better Solutions.™

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

To Enroll, Please Call:
1-800-939-4170
Or Visit:
[https://app.idx.us/account-
creation/protect](https://app.idx.us/account-creation/protect)
Enrollment Code: <<XXXXXXXX>>

October 12, 2022

NOTICE OF <<Variable Header>>

Dear <<Name 1>> <<Name 2>>:

Lindberg & Ripple is writing to inform you of an event that may impact the security of some of your information. Although we are unaware of any attempted or actual misuse of your information, we are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? On or around December 14, 2021, Lindberg & Ripple identified suspicious activity related to an employee's email account. Upon learning of the suspicious activity, we immediately took steps to secure the email account and launched an investigation to determine the nature and scope of the event. The investigation confirmed that an unknown actor had access to two email accounts, one between November 24, 2021 and December 14, 2021 and another for a limited time period prior to April 18, 2021. The investigation could not determine what emails, if any, the unknown actor accessed. In an abundance of caution, we worked with specialists to perform a comprehensive programmatic and manual review of the information stored in the email accounts at the time of event to identify the types of information contained within the accounts and to whom the information related. On April 29, 2022, this extensive review identified certain customer and/or employee information was present within the records. We then conducted a thorough review of our records to confirm the identities and contact information for potentially affected individuals. This review was completed on or around September 23, 2022.

What Information Was Involved? We determined the following types of information relating to you were present in the impacted email accounts: name and <<Data Elements>>. There is no indication that the unknown actor misused this information, and we are providing this notice in an abundance of caution.

What We Are Doing. We take this event and the security of your information seriously. Upon learning of this event, we immediately took steps to secure the affected email accounts. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards to further secure the information in our systems. We also notified state regulators, as required. Although we are unaware of any misuse of your information as a result of this event, we are offering you access to <<12/24>> months of complimentary credit monitoring and identity restoration services through IDX.

What You Can Do. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Protect Personal Information*. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity and to detect errors. You may also enroll in the complimentary credit monitoring services described above. Enrollment instructions are enclosed with this letter.

For More Information. If you have additional questions, please call our dedicated assistance line at 1-800-939-4170, Monday through Friday (excluding U.S. holidays), during the hours of 9:00 a.m. to 9:00 p.m., Eastern Time. You may also write to Lindberg & Ripple at 29 South Main St., Suite 311, West Hartford, CT 06107.

We sincerely regret any inconvenience or concern this event may cause.

Sincerely,

Nancy Shepard

Nancy Shepard
Managing Principal and Chief Operating Officer

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring and Identity Protection Services

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the enrollment deadline is January 12, 2023.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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 one-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 credit 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, 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 a 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

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.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus 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 credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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/>.

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 Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 21 Rhode Island residents impacted by this event.