OCTOBER 23, 2020

Lycoming-Clinton Joinder Board

Notice of Data Security Incident

To Whom It May Concern:

On August 10, 2020, while we were investigating a security incident, we became aware of another security incident that involved unauthorized access to three Lycoming-Clinton Joinder Board ("LCJ") employee email accounts. On September 10, 2020, we learned that the incident may have exposed personal information maintained by LCJ to unauthorized access.

On October 23, 2020, we mailed notifications to individuals whose protected health information and/or personally identifying information could have been accessed without authorization as a result of the incident. Unfortunately, we did not have sufficient contact information to provide written notice to some individuals. With regard to those individuals for whom we did not have sufficient contact information, we are following up by posting this notice on our website and providing our toll-free call center telephone number below. This number can be called to determine whether an individual's personal information was included in the email boxes that were impacted by this incident.

We are providing this notice on our website as a precautionary measure to inform potentially affected individuals of the incident and of protective steps that can be taken. We recommend that you closely review the information provided below for some steps that you may take to protect yourself against potential misuse of your information.

What Happened

On June 23, 2020, we learned that a number of emails had been sent without authorization from an LCJ email account. As soon as we learned about this, we launched an investigation to understand what happened and, more importantly, to prevent something like this from happening again. We also engaged legal counsel with expertise in cyber law – who then engaged a digital forensics company – to assist with our investigation. We provided notice of that incident to affected individuals on September 8, 2020 and posted a notice on our website (https://www.joinder.org/INCIDENTNOTICE.pdf).

On August 10, 2020, during the course of our investigation of the first incident and while instituting remedial measures, we experienced a second incident of emails being sent from LCJ employee email accounts without authorization. We immediately began investigating this second incident and determined that it involved unauthorized intermittent access to three LCJ email accounts between August 5, 2020 and August 10, 2020. While there were similarities between the June 23, 2020 incident and the August 10, 2020 incident, we were unable to confirm whether the incidents were related and from the same attacker.

What Information Was Involved

Once we determined that there had been unauthorized access to the accounts, and because we could not identify what specific information may have been accessed or taken, we reviewed the entire contents of each email box to find out what information was in each email, who may have been affected, and where those people resided. The affected data varied but may have included an individual's name, address, date of birth, medical record or health insurance number, medical history (including diagnoses, substance abuse, lab tests and results, mental or physical health evaluations, and treatment or provider information), costs of care, or circumstances of abuse. For some, but not all, persons, their Social Security number may have also been included.

What We Are Doing About It

When we discovered this incident, we immediately reset the account passwords and worked with technology experts to monitor our systems. To further enhance email and network security, and to help prevent similar occurrences in the future, we have taken the following steps:

1. Increased password complexity;
2. Added two-factor authentication for remote access;
3. Training staff on procedures for saving sensitive data in a new secure data file;
4. Enhancing our cyber training and, in particular, increasing staff education on the risks associated with sharing personal information through email and using alternative, secure methods;
5. Developing and implementing policies and procedures to regularly and securely delete personal information from email and the network; and
6. Restricted access to our network to only those users located in the United States.

In addition, consistent with our compliance obligations and responsibilities, we are providing notice of this incident to appropriate federal and state regulators, including the U.S. Department of Health and Human Services and on our website.

What You Can Do

Out of an abundance of caution, we recommend that you remain vigilant to the possibility of fraud and identity theft by monitoring your account statements, health insurance Explanation of Benefits and other medical insurance statements, and free credit reports for any unauthorized activity. You should report any incidents of suspected identity theft to your local law enforcement and state Attorney General. Information on additional ways to protect your information, including how to obtain a free credit report and free security freeze, can be found at the end of this notice.

If you did not receive written notice regarding this incident, but think that your information, or your relative's information, may have been included in the breach, please call our toll free hotline number 1-800-525-7938, Monday through Friday, from 8:00 a.m. to 4:30 pm EST until January 21, 2021.

We sincerely apologize for any inconvenience this incident may cause. The privacy and security of your information is very important to us and we remain committed to doing everything we can to maintain the confidentiality of your information.

Very truly yours,

Keith Wagner,
Executive Director
Board Secretary
MH/ID Administrator

Mark Egly,
CYS Administrator

MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the consumer reporting agencies listed below and the Federal Trade Commission (FTC) by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.consumer.ftc.gov/features/feature-0014-identity-theft. The FTC's address is: Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You have the ability to place a security freeze on your credit reports by contacting the following agencies.

National Credit Reporting Agencies Contact Information

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com

You also may request a security freeze be added to your credit report at Experian's online Freeze Center, www.experian.com/freeze/center.html, by phone at 1-888-EXPERIAN (1-888-397-3742), or by mail to Experian Security Freeze, P.O. Box 9554, Allen, TX 75013. More information on a security freeze can be found below.

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain your credit reports from each of the national consumer reporting agencies. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies listed above. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report.

If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically, which can help spot and address problems quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them at the information provided above.

Fraud Alerts

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Security Freeze

You have the ability to place a security freeze on your credit report at no cost to you. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. 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; (5) a legible copy of a government-issued identification card, (6) proof of current address, such as a legible copy of a recent utility bill or bank or insurance statement, (7) a legible copy of a recent W-2, pay stub, or Social Security card, and (8) if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. **Under federal law, you cannot be charged to place, lift, or remove a security freeze.**

After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place, you will need it if you choose to lift the freeze. If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

Additional Helpful Information

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them at the information provided above.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.