Good day,

Pursuant to the Personal Information Protection Act (PIPA), Md. Code Ann. Comm. Law 14-3504, we are submitting an electronic copy of the notice provided by US mail today to one (1) Maryland resident potentially affected by a data breach experienced by our client, Our Community Credit Union. We attached a sample copy of the notice provided, which describes the personal information compromised. This incident arose from a business email compromise incident that likely resulted from a phishing attack. The company reviewed system configurations to ensure MFA is fully operational, and to enhance protections for accessing M365. The company also is leveraging third party review services, including a gap assessment and incident response procedures.

Please let me know if you have any questions.

Regards,

JL

Joseph Lazzarotti
Attorney at Law*

Jackson Lewis P.C.
Wells Fargo Center
100 South Ashley Drive.
Suite 2200
Tampa, FL 33602
Direct: (908) 795-5205 | Main: (813) 512-3210 | Mobile: (973) 945-8359

200 Connell Drive
Suite 2000
Berkeley Heights, NJ 07922
Main: (908) 795-5200
Joseph.Lazzarotti@jacksonlewis.com | www.jacksonlewis.com

*Currently licensed in NY, NJ, MO (inactive), and KS (inactive)

OURCU
Our Community Credit Union
Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Notice of Data Incident

Dear <<Full Name>>,

We recently experienced a data incident which may have resulted in unauthorized access or acquisition of your personal information. The purpose of this notice is to provide you with important information about the event, our response, and the steps you can take to further protect your information. It's important to note, that we are not aware of any improper use of your personal information and this notice is being sent as a precautionary measure. Please accept our sincere apology and know that the security of your information is of the utmost importance to us.

What Happened
In early April, we discovered a data incident which may have involved your personal information. This was the result of a compromise to an email account of one of our employees which occurred on or about April 3, 2024.

What Information Was Involved
The data elements involved may have included your name, address, phone number, Social Security number, and credit union account number.

What We Are Doing
Upon discovering the incident, we immediately commenced an investigation working with our internal response team and third-party IT service providers to secure our information systems. We also arranged to make available, ID theft and credit monitoring services.

We treat all personal information in a confidential manner and are proactive in the careful handling of such information. Theft of data and similar incidents are difficult to prevent in all instances, however, we have reviewed our systems and continue to make improvements where we can minimize the chances of this happening again. For example, we have changed system passwords, strengthened system authentication, and improved system monitoring.

What You Can Do
While we are unaware of any misuse of your personal information as a result of this incident, included are steps you can take to protect your identity and personal information.

In addition, we are offering identity theft protection services through Equifax at no cost to you. These identity theft protection services include 12 months of identity theft recovery services and credit monitoring. With this protection, you will have access to resources to help you resolve issues if your identity is compromised. Please see the attached sheet for more information, including your activation code. Please note that you must enroll within 90 days of the date of this letter.

For More Information
If you have questions or concerns, please contact us at 800-426-5657**.** We are available any time between Monday - Friday 8:00 AM to 5:30 PM pacific. We sincerely regret that this incident occurred and apologize for any inconvenience it may cause you.

Sincerely,

Ryan C. Drake

EQUIFAX®

<<First Name>> <<Last Name>>
Enter your Activation Code: <<Activation Code>>
Enrollment Deadline: <<Enrollment Deadline>>

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of <<Activation Code>> then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. [2]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. [3]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com [4]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

<u>What You Should Do to Protect Your Personal Information</u>

We recommend you remain vigilant and consider taking the following steps to avoid identity theft, obtain additional information, and protect your personal information:

- Order Your Free Credit Report at www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov. When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize and notify the credit bureaus as soon as possible in the event there are any.

- Place a Fraud Alert on Your Credit File. A fraud alert helps protect you against an identity thief opening new credit in your name. With this alert, when a merchant checks your credit history when you apply for credit, the merchant will receive a notice that you may be a victim of identity theft and to take steps to verify your identity. You also have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can place a fraud alert or request a security freeze by contacting the credit bureaus. The credit bureaus may require that you provide proper identification prior to honoring your request.

  Equifax, P.O. Box 740241, Atlanta, GA 30374, 1-888-298-0045, www.equifax.com,

  Experian, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com,

  TransUnion, P.O. Box 2000, Chester, PA 19016, 1-800-916-8800, www.transunion.com,

- Remove your name from mailing lists of pre-approved offers of credit for approximately six months.

- If you aren't already doing so, please pay close attention to all bills and credit-card charges you receive for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

- The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may also obtain information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General, and/or the Federal Trade Commission ("FTC"). You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC at 1-877-IDTHEFT (1-877-438-4338), or www.ftc.gov/idtheft. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.

- *For Maryland Residents:* You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us.

- *For New York Residents:* You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or https://ag.ny.gov/internet/resource-center; or 2) NYS Department of State's Division of Consumer Protection, (800) 697-1220 or https://dos.ny.gov/consumer-protection.

- *For North Carolina Residents:* You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.