POLSINELLI

900 W. 48th Place, Suite 900, Kansas City, MO 64112 • 816.753.1000

June 30, 2023

VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)

John Formella, Attorney General
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Re: Notification of a Data Security Incident

Dear Attorney General Formella:

We represent Clearwater Credit Union ("Clearwater"), 3600 Brooks Street, Missoula, MT 59801 in connection with an incident that involved certain member information of seven (7) New Hampshire residents. Clearwater is reporting the incident pursuant to N.H. REV. STAT. ANN. § 359-C:20. This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to this submission. While Clearwater is notifying you of this incident, Clearwater does not waive any rights or defenses relating to the incident, this notice, or the applicability of New Hampshire law on personal jurisdiction.

NATURE OF THE INCIDENT

On June 14, 2023, Clearwater was notified by one of its vendors, Alogent Holdings, Inc. ("Alogent"), that unauthorized third parties exploited a previously unknown vulnerability in MOVEit, a file transfer service used by Alogent. Upon discovering the incident, Alogent and Clearwater promptly initiated internal investigations. In addition, Clearwater obtained legal counsel and notified law enforcement. Alogent's investigation determined that at the end of May 2023, the third parties gained unauthorized access to Alogent files stored on MOVEit systems, including certain Alogent files containing Clearwater data. Unauthorized access to Alogent files containing Clearwater's data occurred between May 30, 2023 and May 31, 2023.

On or around June 14, 2023, Alogent provided to Clearwater a list of files containing Clearwater data that were accessed and acquired by the unauthorized third parties. Clearwater reviewed the identified files and determined that they included information such as

.

This incident was limited to unauthorized access to the MOVEit system maintained by Alogent and certain files contained therein, including some Alogent files containing Clearwater data. The incident did not involve unauthorized access to any Clearwater systems or accounts. At this point, Clearwater is not aware of any fraud or identity theft to any individual as a result of this incident.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

Clearwater conducted a comprehensive review of the accessed and acquired files to determine if they contained any personal information. Clearwater determined that the files included the personal information of certain individuals and thereafter worked to locate current contact information for each involved individual. Clearwater notified those individuals, including seven (7) New Hampshire residents, on June 30, 2023. The notification letter includes an offer of complimentary credit monitoring and identity theft protection services for individuals whose personal information was involved in the incident. Enclosed is a sample copy of the notice being sent via first-class United States mail.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, Clearwater promptly notified law enforcement and worked with Alogent to investigate the incident and determine what Clearwater data may have been involved. As discussed above, Clearwater is notifying potentially involved individuals, providing free credit monitoring services, and providing individuals with information on how they can protect themselves against fraudulent activity and identity theft.

CONTACT INFORMATION

Please do not hesitate to contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

Alexander D. Boyd

Enclosure

clearwater
CREDIT UNION

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

June 30, 2023

Dear <<Name 1>>:

Clearwater Credit Union values and respects your privacy, which is why we are writing to advise you of a recent incident at one of our vendors that involved some of your personal information. This letter explains the incident, the steps we have taken in response, and the steps you may take to help protect your information, should you feel it is appropriate to do so.

What Happened?
MOVEit is a popular file transfer service used by government agencies, corporations, financial institutions, and other organizations worldwide. Clearwater does not directly use MOVEit; however, one of our vendors does. On June 14, 2023, we learned that unauthorized third parties exploited a previously unknown vulnerability in MOVEit that allowed those third parties to gain access to files on MOVEit systems at the end of May 2023. An investigation determined that the third parties gained access to certain Clearwater documents between May 30, 2023, and May 31, 2023.

This incident did not involve unauthorized access to any Clearwater systems. Your accounts at Clearwater were not accessed by any unauthorized parties in this incident.

What Information was Involved?
We reviewed the documents acquired by the third party and determined that the documents contained personal information that included your <<Breached Elements>>.

What We Are Doing
We are working closely with our vendor to ensure that they are taking steps to further secure our members' information. Although we are not aware of any fraud or identity theft instances involving your information, we are offering you a complimentary one-year membership to Experian IdentityWorks^{SM} Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on prompt identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you, and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary, , please see the enclosed letter.**

What You Can Do
You can find more information about how to protect yourself against possible identity theft or fraud in the enclosed *Additional Important Information* sheet. In addition to taking advantage of IdentityWorks 3B, we encourage you to familiarize yourself with the best practices described in this enclosure.

For More Information.
We value the trust you place in us to protect your privacy. We take our responsibility to safeguard your personal information seriously, and we apologize for the inconvenience and concern this incident may cause you. For further information and assistance, please contact our incident response center at .

Sincerely,

Jack Lawson
President and CEO

Activating Your Complimentary Credit Monitoring

To help protect your identity, we are offering you a **complimentary** one-year membership to Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **<<Enrollment Deadline>>** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: .
3. PROVIDE the **Activation Code**: **<<Activation Code>>.**

If you have questions about the product, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at . Please be prepared to provide your engagement number <<Engagement Number>> as proof of eligibility for Experian's identity restoration services.

ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP

A credit card is **not** required to enroll for Experian IdentityWorks Credit 3B. You can contact Experian **immediately** regarding any fraud issues and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only. *
- **Credit Monitoring:** Actively monitors Experian, Equifax, and Transunion files for fraud indicators.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at or call to register with the activation code above.

What You Can Do to Protect Your Information
There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report, or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at .

* Offline members will be eligible to call for additional reports quarterly after enrolling.
** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Important Information

As a precautionary measure, we recommend that you do the following to remain vigilant and protect yourself against potential fraud and/or identity theft.

- Review your account statements and credit monitoring reports closely.
- If you detect suspicious account activity, promptly notify the financial institution or company that maintains your account.
- Report any fraudulent activity or any suspected identity theft incidents to proper law enforcement authorities, including the police, your state's attorney general, and the Federal Trade Commission ("FTC").
- Review the FTC's tips on fraud alerts, security/credit freezes, and the steps you can take to avoid identity theft.

For more information and to contact the FTC please:

- Visit www.ftc.gov/idtheft;
- Call 1-877-ID-THEFT (1-877-438-4338); or
- Write to the FTC at Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

Credit Reports
You may obtain a free copy of your credit report from each of the three national credit reporting agencies once every 12 months by:

- Visiting www.annualcreditreport.com;
- Calling toll-free 1-877-322-8228; or by
- Completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies as follows:

Equifax	**Experian**	**TransUnion**
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts
You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. 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.

Credit and Security Freezes
You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze can be placed without any charge and is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

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

This notification was not delayed by law enforcement.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, http://www.marylandattorneygeneral.gov/.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; https://ag.ny.gov/consumer-frauds/identity-theft; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Rhode Island Residents: We believe that this incident affected **five (5)** Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).