July 18, 2023

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
attorneygeneral@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General Formella:

We are writing to notify you of a data security incident involving seven (7) New Hampshire residents.

IDENTIFICATION OF PARTIES

A third-party vendor of Workers, myCUmortgage, LLC, informed the Credit Union that one of their third-party vendors, Mortgage Industry Advisory Corporation ("MIAC") experienced a ransomware attack which resulted in unauthorized acquisition of personal information for thirty-two (32) Workers members, including seven (7) New Hampshire residents.

NATURE OF THE DATA SECURITY INCIDENT

Workers received a notification from Tonya M. Coon, President of myCUmortgage, LLC, 3560 Pentagon Boulevard, Suite 301, Beavercreek, OH, 45431 on June 30, 2023. The notification states that MIAC notified them of a ransomware attack on April 15, 2023, which resulted in unauthorized acquisition of personal information of Workers members, including

.

Per the notification letter received, MIAC's investigation is ongoing, and they have not yet stated whether the unauthorized access involved unencrypted data. We are informing you of this breach by our third-party vendor, as it poses potential risk of fraud or identify theft to our members of the Credit Union who were impacted.

MIAC is not aware of any misuse of the personal information impacted as of the date of the notification to Workers. Workers is also not aware at this time of any misuse of the personal information as a result of this incident.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

The number of affected New Hampshire residents whose personal information was accessed, as known at the time of this notification, is seven (7). MIAC will begin mailing notices on July 24th. A copy of the notice is included with this communication.

STEPS TAKEN OR TO BE TAKEN RELATING TO THE INCIDENT

Upon notification of this incident, Workers initiated its Incident Response Team and began taking appropriate incident response steps. The Board of Directors was also notified.

The notification to Workers indicated that MIAC is continuing its forensic investigation and has implemented additional technical safeguards to help prevent a similar incident in the future.

Workers continues to monitor the incident through contact with the vendor.

CREDIT MONITORING SERVICES

MIAC is offering complimentary credit monitoring services through IDX to impacted members in compliance with state law. Instructions for enrolling in the services is being provided as part of the notifications being mailed to the Workers members who were impacted.

If you have any questions or need further information, please contact me at your convenience.

Sincerely,

Patricia North-Martino
VP, Senior Information Security Risk Officer

Enclosures:

1. myCU – MIAC Letter

<<Return Mail Address>>

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>> <<Date>>
<<City>>, <<State>> <<Zip>>
<<Country>>

NOTICE OF / <<DATA BREACH/SECURITY INCIDENT>>

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

Mortgage Industry Advisory Corporation ("MIAC") is writing to notify you of a recent incident that may affect the privacy of some of your personal information. MIAC provides loan valuation and other financial analytics services to <<Data Owner>> and received your information in connection with these services. <<Data Owner>> received certain loan application information from <<credit union>> in anticipation of servicing your loan. If your mortgage loan was funded, <<Data Owner>> also services your mortgage account. This security incident did not involve unauthorized access to any <<Data Owner>> systems or any systems at your credit union. MIAC takes the protection of your information very seriously, and although we have no evidence of identity theft or fraud as a result of this incident, this letter provides information about the incident, our response, and steps you may wish to take to protect against possible misuse of your information.

Commented [AB1]: myCUmortgage

What Happened? On April 6, 2023, MIAC became aware of a cyberattack on our systems. We immediately took steps to secure our systems and began an investigation into the nature and scope of the event. The investigation determined that in connection with the incident there was unauthorized access to certain systems in our environment, and as a result, certain data stored on our systems were subject to unauthorized acquisition between [DATE – DATE]. We then undertook a comprehensive review of the affected data to confirm what information was impacted. On [DATE], we notified <<Data Owner>> that information pertaining to them may be affected, and on [DATE identified PII for particular client] identified information relating to you was contained in the affected files. To be clear, there was not a security incident at <<Data Owner>> or at your credit union. At this time, we are unaware of any actual or attempted misuse of your information as a result of this incident.

What Information Was Involved? The investigation determined your name and the following types of data were present in the files that were identified as acquired without authorization: [DATA ELEMENTS].

What We Are Doing. We take this incident and the security of information in our care seriously. Upon learning of this incident, we immediately secured our environment, investigated to determine the nature and scope of the incident, and notified law enforcement. We have also implemented additional technical safeguards to help prevent a similar incident in the future.

Although we are unaware of any identity theft or fraud resulting from this incident, MIAC is offering you access to [12/24] months of complimentary credit monitoring and identity protection services through [Vendor]. Details of this offer and instructions on how to enroll in the services may be found in the attached *Steps You Can Take to Protect Personal Information*. If you would like to enroll in these services you will need to follow the attached instructions, as we are unable to enroll you automatically.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud over the next twelve to by reviewing your account statements and immediately report any suspicious activity or incidents of suspected identity theft or fraud to your bank or other financial institution(s). Additional information may be found in the attached *Steps You Can Take to Protect Personal Information*.

For More Information. If you have questions regarding this incident, you may contact our dedicated assistance line at [call center number] between the hours of X:00am and X:00pm Eastern. You may also write to MIAC at [ADDRESS].

Sincerely,

[MIAC CONTACT]

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

[Enrollment Instructions]

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. MIAC recommends consumers periodically obtain their credit reports from each nationwide credit reporting agency and have information relating to any fraudulent transactions deleted. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information, depending on whether the request is made online, by phone, or by mail:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number or copy of Social Security card;
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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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	1-800-916-8800
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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud and obtain a copy of it. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant 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, D.C. 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 https://www.marylandattorneygeneral.gov/. MIAC is located at 521 5th Ave., 6th Floor, New Yok, NY 10175.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately [#] Rhode Island residents that may be impacted by this event.