MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

September 5, 2023

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Supplemental Notice of Data Event

To Whom It May Concern:

We represent Mortgage Industry Advisory Corporation ("MIAC") located at 521 5th Ave, 6th Floor, New York, NY 10175, and are writing to supplement our notice to your office of an incident that may affect the security of certain personal information relating to an additional seven (7) New Hampshire residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, MIAC does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On April 6, 2023, MIAC became aware of a cyberattack on its computer systems. MIAC immediately took steps to secure its systems and began an investigation into the nature and scope of the event. Third-party forensic, and other, external specialists were brought in to assist with this process. Through this investigation, MIAC determined that it was the victim of a ransomware attack and that an unauthorized actor accessed and exfiltrated certain files stored on its systems between April 5, 2023, to April 6, 2023. MIAC then undertook a comprehensive review of the affected data to confirm what information was impacted, and notified its impacted clients, who own the data at issue. On August 17, 2023, MIAC determined that information related to certain customers of MIAC's client, PHH Mortgage Corporation ("PHH") was included in the impacted files. MIAC is unaware of any actual or attempted misuse of information as a result of this incident.

The information that could have been subject to unauthorized access includes
.

Notice to New Hampshire Residents

On September 5, 2023, MIAC provided written notice of this incident to approximately seven (7) New Hampshire residents at the direction of PHH, the entity that owns the data at issue.

Written notice was 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, MIAC moved quickly to investigate and respond to the incident, assess the security of its systems, and identify potentially affected information. Further, MIAC notified federal law enforcement regarding the event. MIAC is also working to implement additional technical safeguards to further increase the security of its environment. MIAC is providing access to credit monitoring services for through IDX, to individuals whose personal information was affected by this incident, at no cost to these individuals.

Additionally, MIAC is providing impacted individuals with guidance on how to better protect against identity theft and fraud. MIAC is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, 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 Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

MIAC is providing written notice of this incident to relevant state regulators as necessary at the direction of affected data owners.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at .

Very truly yours,

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/dtg
Enclosure

EXHIBIT A

MIAC Analytics™
P.O. Box 989728
West Sacramento, CA 95798-9728

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

September 5, 2023

NOTICE OF <<DATA BREACH/SECURITY INCIDENT>>

Dear <<FIRST NAME>> <<LAST NAME>>:

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 mortgage warehouse lenders including Texas Capital Bank ("TCB"), a business partner of PHH Mortgage Corporation ("PHH"). MIAC received your information in connection with providing services to TCB. MIAC takes the protection of your information very seriously. Although we have no evidence of actual or attempted misuse, identity theft or fraud related to your information 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 misuse of your information.

What Happened? On April 6, 2023, MIAC became aware of a cyberattack on our systems. MIAC immediately took steps to secure its systems and began an investigation into the nature and scope of the incident. The investigation determined that in connection with the incident there was unauthorized access to certain systems in MIAC's environment, and as a result, certain data stored on MIAC's systems were subject to unauthorized acquisition on April 6, 2023. MIAC then undertook a comprehensive review of the affected data to confirm what information was impacted. The investigation continued through August 17, 2023, to confirm what information related to PHH was impacted so MIAC could begin to obtain address information for affected individuals in order to provide an accurate notice to impacted parties.

TCB is PHH's business partner. TCB uses MIAC's financial analytical services. MIAC received PHH customer information in connection with these services. MIAC's investigation revealed that PHH customer information was impacted by the incident. PHH was notified on June 21, 2023, that certain PHH customer information was acquired by an unauthorized actor in connection with this incident.

What Information Was Involved? The investigation determined your
were present in the files that were identified as acquired without authorization.

What We Are Doing. We take this incident and the security of information in our care seriously. Upon learning of this incident, MIAC promptly secured its environment, investigated to determine the nature and scope of the incident, and notified law enforcement. MIAC 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 months of complimentary credit monitoring and identity protection services through IDX, a ZeroFox Company, the data breach and recovery services expert. 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. While MIAC is unaware of any actual or attempted misuse of your information as a result of this incident, we encourage you to remain vigilant against incidents of identity theft and fraud over the next twelve to twenty-four months 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). You may review the information contained in the attached "Steps You Can Take to Help Protect Your Information." You may also activate your access to IDX identity and credit monitoring services we are making available to you. There is no charge to you for the cost of these services; however, you will need to follow the instructions below to activate your enrollment in this service.

For More Information. If you have questions regarding this incident, you may contact a dedicated assistance line that PHH has set up with MIAC at 1-888-567-0238 between the hours of 9:00am and 9:00pm Eastern. You may also write to MIAC at 521 Fifth Ave., 6th Floor, New York, NY 10175.

Sincerely,

Mortgage Industry Advisory Corporation

Steps You Can Take To Protect Personal Information

Enroll in Monitoring Services

1. Website and Enrollment. Go to and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is .

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 1-888-567-0238 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. 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 Massachusetts residents, 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.

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, you may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office. 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. you may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office the

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 7 Rhode Island residents that may be impacted by this event.