CONSTANGY BROOKS, SMITH & PROPHETE LLP

Aubrey Weaver, Partner
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, PA 19103
aweaver@constangy.com
Mobile: 941.875.5335

June 28, 2023

VIA U.S. MAIL
Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident - Update

Dear Attorney General John Formella:

We are writing to provide an update to our letter dated April 20, 2023, regarding the recent data security incident experienced by IMA Financial Group, Inc. ("IMA"). This update is being sent on behalf of IMA and certain of its clients, listed below, because personal information for additional New Hampshire residents has been identified as potentially involved in the data security incident previously reported by IMA.

1. Nature of the Security Incident

As you know, on October 19, 2022, IMA learned of unusual activity involving certain systems in its network. Upon discovering this activity, IMA's internal security teams took immediate steps to secure its network. IMA also engaged a team of leading external cybersecurity experts to assist in its response and conduct an investigation to determine what happened and what information may have been involved. IMA's investigation revealed that on October 19, 2022, certain IMA data may have been accessed or acquired without authorization in connection with the incident.

As a result, IMA launched a comprehensive review of the potentially affected data with the assistance of external experts. This review concluded on March 10, 2023 and revealed that some individuals' information may have been contained therein. IMA thereafter worked to provide notice to its clients and gather outstanding information needed to provide individual notification.

2. Number of New Hampshire Residents Affected

On June 27, 2023, IMA concluded that the notification population included a total number of 39 New Hampshire residents. IMA provided individual notifications on a rolling basis between April 19, 2023, and June 29, 2023, via the attached notification letter template or a substantially similar version thereof. The potentially affected personal information for New Hampshire residents includes individuals'

3. Steps Taken Relating to the Incident

As soon as IMA discovered this unusual network activity, it took steps to secure its systems and launched an investigation to determine what happened and whether personal information had been accessed or acquired without authorization. IMA has implemented additional safeguards to help ensure the security of its systems and to reduce the risk of a similar incident occurring in the future.

IMA has established a toll-free call center through IDX to answer questions about the incident and address related concerns. In addition, IMA is offering of complimentary credit and identity monitoring services to the potentially affected individuals.

4. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me.

Sincerely,

Aubrey L. Weaver
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Attachment: Sample Notification Letter

4145 SW Watson Avenue,
Suite 400
Beaverton, OR 97005

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

June 28, 2023

Subject: Notice of Data <<Variable 1: Security Incident or Breach>>

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a data security incident that may have involved your personal information. At IMA Financial Group, Inc. ("IMA") and its subsidiaries, we take the privacy and security of individuals' information very seriously. If you are not familiar with IMA, we are an insurance broker/service provider that works with your current or former employer, <<Variable 2: Employer>>. This letter provides steps you can take to protect your information, including enrolling in the complimentary credit monitoring and identity protection services we are making available to you.

What Happened? On October 19, 2022, IMA learned of unusual activity involving certain systems in our network. Upon discovering this activity, our internal security teams took immediate steps to secure our network. We also engaged a team of leading external cybersecurity experts to assist in our response and conduct an investigation to determine what happened and what information may have been involved. Our investigation revealed that on October 19, 2022, certain IMA data may have been accessed or acquired without authorization in connection with the incident. As a result, we launched a comprehensive review of the potentially affected data. Our review concluded on March 10, 2023, and identified some of your information within the potentially affected dataset. We subsequently provided notice to your employer and worked with them to issue this letter.

What Information Was Involved? The potentially affected information includes your <<Variable 3: Data Elements>>.

What Are We Doing? As soon as we discovered this incident, we took the steps described above. We have also implemented additional safeguards to help ensure the security of our network environment and to reduce the risk of a similar incident occurring in the future.

Additionally, to help relieve concerns and to help protect your identity following this incident, IMA is offering you < of complimentary credit monitoring and identity protection services through IDX, a data breach and recovery services expert. The IDX services include: months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. The deadline to enroll is September 28, 2023.

What Can You Do? We recommend that you activate your complimentary IDX services using the enrollment code provided above. A description of the services available upon enrollment is included with this letter. We also recommend that you review the guidance included with this letter about steps you can take to protect your information.

For More Information: If you have questions or need assistance, please contact IDX at , Monday through Friday from 8 am to 8 pm Central Time, excluding major U.S. holidays. IDX representatives are fully versed on this incident and can answer any questions you may have regarding the protection of your information.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

IMA Financial Group, Inc.
430 E. Douglas, Suite 400
Wichita, KS 67202

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800525-6285
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

Fraud Alert: 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 one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting act.pdf.

IDX Identity Protection Services

1. **Website and Enrollment**. Go to follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

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. *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 1-888-404-4885 to speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help. If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

IDX Identity will include <<12 / 24 >> months of enrollment into the following service components:

1. SINGLE BUREAU CREDIT MONITORING - Monitoring of credit bureau for changes to the member's credit file such as new credit inquiries, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.
2. CYBERSCAN - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like Social Security numbers, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.
3. IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to $1,000,000, with no deductible.
4. FULLY-MANAGED IDENTITY RECOVERY - IDX's fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned ID Care Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.