Clark Hill

Melissa K. Ventrone
T (312) 360-2506
F (312) 517-7572
Email:mventrone@ClarkHill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

May 27, 2022

Via Electronic Mail

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
consumer@ag.iowa.gov

To Whom It May Concern:

We represent Hawkeye Financial Group ("HFG") with respect to a data security incident involving potential exposure of certain personally identifiable information ("PII") described in more detail below. HFG is a financial planning group in Wellman, Iowa. HFG is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident in the future.

1. Nature of security incident.

On December 21, 2021, HFG discovered suspicious activity associated with one of its employees' email accounts. As soon as HFG learned of the suspicious activity, it began an investigation to determine what occurred and whether any data was at risk. The investigation found unauthorized access to one email account between December 19-21, 2021. HFG then hired an independent firm to conduct an in-depth review of the email account to determine what personal information may have been present in the affected account. This review was completed on April 26, 2022, at which point it was determined that personal information for some HFG clients were present in the account at the time of the unauthorized access. Potentially affected information may include some client's first and last names, addresses, dates of birth, driver's license numbers, Social Security numbers, financial information, and for a small subset of individuals, limited medical information.

2. Number of residents affected.

Seven hundred sixty-five (765) Iowa residents may have been affected and were notified of the incident. A notification letter was sent to the potentially affected individuals on May 27, 2022 (a copy of the form notification letter is enclosed as Exhibit A).

3. Steps taken in response to the incident.

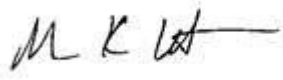
HFG took steps to address this incident and to prevent similar incidents in the future, including changing all passwords, deploying multi-factor authentication for remote access, and retraining staff on recognizing and responding to suspicious computer activity. Affected individuals were offered 12 months of credit monitoring and identity protection services from IDX, the data breach and recovery services expert.

4. Contact information.

HFG takes the security of the information in its control seriously and is committed to ensuring it is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at mventrone@clarkhill.com or (312) 360-2506.

Sincerely,

CLARK HILL



Melissa K. Ventrone
Member

cc: Daisy Dai ddai@clarkhill.com

Hawkeye Financial Group

EXHIBIT A

10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

HAWKEYE FINANCIAL GROUP
"For Those Serious About Their Future."

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

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

May 27, 2022

NOTICE OF DATA SECURITY INCIDENT

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

We wanted to let you know about a data security incident that may have impacted your personal information. Hawkeye Financial Group ("HFG") takes the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains details regarding the incident, and resources we are making available to help you protect your personal information.

What happened:

On December 21, 2021, we discovered suspicious activity associated with one of our employee's email accounts. As soon as we learned of the incident, we began an investigation to determine what occurred and whether any data was at risk. Unfortunately, this investigation found unauthorized access to one email account. We then hired an independent firm to conduct an in-depth review of the email account to determine what personal information may have been present in the affected account. This review was completed on April 26, 2022, at which point we determined that some of your personal information was present in the affected email account at the time of unauthorized access.

What information was involved:

Information stored in our systems may include <<variable text>>.

What we are doing:

We have taken steps to prevent a similar incident in the future, including changing all passwords, deploying multi-factor authentication for remote access, and retraining staff on data security best practices. We have also arranged for you to receive credit monitoring and identity protection services from the data breach and recovery services expert. IDX identity protection services include: <<12/24 months>> of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What you can do:

It is always a good idea to remain vigilant for incidents of identity theft or fraud, and to review your bank account and other financial statements as well as your credit reports for suspicious activity. We also encourage you to contact IDX with any questions and to take full advantage of the IDX service offering. Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information:

If you have any questions or concerns, please call 1-800-939-4170 Monday through Friday from 8 am - 8 pm Central Time. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you. Please note the deadline to enroll is August 27, 2022.

Sincerely,

Justin Ryan

RECOMMENDED STEPS TO HELP PROTECT YOUR INFORMATION

1. **Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and 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. Note: You must have 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 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Watch for Suspicious Activity. 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.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Security Freeze. You may place a free credit freeze for children under age 16. By placing a security freeze, someone who fraudulently acquires your child's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact the three national credit reporting bureaus listed below to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your child's credit files

6. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
P.O. Box 105069
Atlanta, GA 30348-5069
Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-836-6351
www.equifax.com/personal/credit-report-services

Experian Fraud Reporting and
Credit Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion Fraud Reporting
P.O. Box 2000
Chester, PA 19022-2000
TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094
1-800-680-7289
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You 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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_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.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.