



Donna Maddux
Partner
4800 Meadows Road, Suite 300
Lake Oswego, Oregon 97035
503.312.6251
dmaddux@constangy.com

June 24, 2024

VIA ONLINE SUBMISSION

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete LLP (“Constangy”) represents HFM Investment Advisors, LLC (“HFM”), a financial planning and investment advisory firm in New Jersey, in connection with the data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland’s data breach notification statute.

1. Nature of the Security Incident

On February 6, 2024, HFM became aware of unusual activity associated with an employee’s email account. In response, HFM took immediate steps to secure its email environment and promptly launched an investigation. The investigation conducted by third-party cybersecurity experts determined that an unknown actor accessed and acquired certain data without authorization.

Following a forensic investigation and data mining of the impacted account, on June 4, 2024 HFM confirmed that certain personal information may have been impacted and then took steps to effectuate notification to potentially impacted individuals as quickly as possible. Please note that there is currently no evidence of fraud or misuse of any of the data, only evidence that data was acquired without authorization.

2. Number of Affected Maryland Residents & Information Involved

The incident involved personal information for seventeen (17) Maryland residents. The information involved in the incident for the affected Maryland residents may have included name, Social Security number and driver's license.

3. Notification to the Affected Individuals

On June 24, 2024, a notification letter was sent to the affected Maryland residents by USPS First Class Mail. The notification letter provides resources and steps these individuals can take to help protect their information. The notification letter also offers the individuals the opportunity to enroll in 12 months of complimentary identity protection services, including credit monitoring, and identity remediation services, as well as access to a call center, should the individuals have questions about the incident. A sample notification letter sent to the impacted individuals is included with this correspondence.

4. Steps Taken Relating to the Incident

In response to the incident, HFM retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. HFM also implemented additional security measures to further harden its email environment in an effort to prevent a similar event from occurring in the future.

Finally, HFM is notifying the affected individuals and providing them with steps they can take to protect their personal information as discussed above. HFM has also established a toll-free call center through Epiq, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns.

5. Contact Information

HFM remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Donna Maddux at dmaddux@constangy.com.

Sincerely,



Donna Maddux
Constangy, Brooks, Smith & Prophete, LLP

Encl.: Sample Notification Letter



25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

To Enroll, Please Call:

866.622.9303

Or Visit:

app.identitydefense.com/enrollment/activate/hfm

Enrollment Code: <<Activation Code>>

<<Date>>

Subject: Notice of Data <<Variable Data 1>>

Dear <<Full Name>>,

We are writing to inform you of a data security incident that may have involved your personal information. Please read this letter carefully as it contains details about the incident and resources you can utilize to protect your information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services.

Please know that we have always prioritized the security and confidentiality of our clients' information and have implemented robust measures to protect it. However, in today's increasingly digital world, no system is entirely immune to breaches. We sincerely apologize for any inconvenience this incident may cause and want to assure you that we undertook immediate steps to address the situation. Additionally, we are enhancing our cybersecurity protocols to reduce the likelihood of future incidents and better safeguard your personal information. We remain committed to maintaining your trust and confidence, and we appreciate your understanding and continued support.

What Happened? On February 6, 2024, HFM discovered unusual activity associated with an employee's email account. The investigation determined that an unknown actor acquired certain data without authorization on or about February 6, 2024. We then conducted a comprehensive review of the affected data to determine whether personal information may have been involved. After a thorough review of the impacted data, on June 4, 2024, it was determined that some of your personal information was present in the impacted data set. We then took steps to notify you of the incident as quickly as possible.

What Information Was Involved? The information involved may include your name and your << Breached Elements>>.

What We Are Doing. As soon as we discovered the incident, we took the steps described above. We also implemented additional measures to reduce the risk of a similar incident occurring in the future.

We are also offering you the ability to enroll in <<CM Duration>> months of complimentary CyEx credit monitoring and identity protection services through Epiq, a global technology services leader.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the CyEx identity protection services, which are offered at no cost to you.

To enroll in CyEx Identity Defense visit app.identitydefense.com/enrollment/activate/hfm

1. Enter your unique Activation Code listed at the top of this letter
Enter your Activation Code and click 'Redeem Code'.
2. Create Your Account
Enter your email address, create your password, and click 'Create Account'.
3. Register
Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. Complete Activation
Click 'Continue to Dashboard' to finish enrolling.

Please note the deadline to enroll in these complimentary services is <<Enrollment Deadline>>. Please do not discard this letter, as you will need the Activation code provided above to access services.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 888-498-6103, Monday through Friday, 9 am to 9 pm Eastern time. Epiq representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

HFM values its clients and the relationships we have established throughout the years. We deeply regret any worry or inconvenience that this may cause you.

Sincerely,

HFM Investment Advisors, LLC

ADDITIONAL STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR 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 monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. 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). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

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 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 this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. 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>. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right 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. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

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.

Additional Information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov; <https://oag.dc.gov/>

California: The California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; <http://oag.ca.gov/>

Maryland: The Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us; <https://www.marylandattorneygeneral.gov/>

North Carolina: The North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; <https://ncdoj.gov/>

New York: The New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/>

Rhode Island: The total number of Rhode Island residents receiving notification of this incident is <<RI Count>>. The Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, <http://www.riag.ri.gov>

Texas: The Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/

Vermont: The Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; ago.info@vermont.gov; <https://ago.vermont.gov/>