



Lauren Godfrey
322 North Shore Drive,
Building 1B, Suite 200
Pittsburgh, PA 15212
lgodfrey@constangy.com
973.462.9521

January 6, 2025

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: Idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP, represents Heard, McElroy, & Vestal LLC (“HMV”) in relation to a data security incident. HMV takes the protection of all information within its possession very seriously and has taken measures to reduce the likelihood of a similar incident reoccurring. We are writing to notify your office of an incident that may affect the security of certain personal information relating to one Maryland resident.

1. Nature of the Security Incident

On or around July 17, 2024, HMV identified unusual login activity to its document imaging solution. HMV immediately began investigating and enlisted the assistance of cybersecurity and other technical experts to assist with identifying what happened and whether personal information in HMV’s possession was accessed without authorization. HMV identified that information related to certain HMV clients was downloaded without authorization. HMV then conducted a comprehensive review of all potentially affected information. During a thorough review of the information, HMV determined that certain personal information was contained in the potentially affected data. HMV then took steps to locate contact information needed to effectuate notification to such individuals. This process was completed on December 12, 2024, and notice was provided promptly thereafter.

The potentially affected information varies for each individual, but may have included the individual’s name and Social Security number.

2. Number of Maryland Residents Affected

On January 6, 2025, HMV notified one Maryland resident within the potentially affected population, via USPS First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

As soon as HMT learned of the unusual network activity, it took steps to secure its systems and launched an investigation to learn more about what happened and what information could have been affected. HMT 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.

HMT is providing those whose Social Security number was involved with identity protection services through IDX. The IDX identity protection services include CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. In addition, HMT has established a toll-free call center through IDX to answer questions about the incident and address related concerns.

Additionally, HMT is providing impacted individuals with guidance on how to better protect against identity theft and fraud. HMT 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.

4. Contact Information

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

Sincerely,

Lauren D. Godfrey

Lauren D. Godfrey
Partner, Constangy Cyber Team

Attachment: Sample Notification Letter

HMV
CERTIFIED PUBLIC ACCOUNTANTS
P.O. Box 989728
West Sacramento, CA 95798-9728

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

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

January 6, 2025

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

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

We are writing to inform you of a data security incident that may have affected your personal information. At Heard, McElroy & Vestal, LLC (“HMV”), we are committed to maintaining our clients’ trust and demonstrating our commitment to the privacy and security of all information in our possession. That is why we are writing to notify you of this incident, to offer you complimentary credit monitoring and identity theft restoration services, and to inform you about steps that can be taken to help safeguard your personal information.

What Happened: On or around July 17, 2024, HMV identified unusual login activity to its document imaging solution. We immediately began investigating and enlisted the assistance of cybersecurity and other technical experts to assist with identifying what happened and whether personal information in HMV’s possession was accessed without authorization. HMV identified that information related to certain HMV clients was downloaded without authorization. HMV then conducted a comprehensive review of all potentially affected information. During a thorough review of the information, we determined that some of your personal information was contained in the potentially affected data. HMV then took steps to locate contact information needed to effectuate notification to such individuals. At the conclusion of this process on December 12, 2024, HMV arranged for notification to potentially affected individuals.

In response to the incident, we have taken immediate steps to secure our systems and will continue to evaluate additional protections that can be put into place to supplement our existing security policies and procedures as the investigation continues.

What Information Was Involved: The information affected may have included the information reflected on your tax return and related documents, including your name and <<Variable Data 2>>.

What We Are Doing: Upon discovering this incident, in addition to taking the steps described above, we immediately notified the Federal Bureau of Investigation (“FBI”) and the Internal Revenue Service (“IRS”) in an effort to prevent the processing of unauthorized tax returns. We will continue to provide relevant information about this incident and whatever cooperation is necessary to hold the perpetrator(s) accountable.

In addition, we are offering identity protection services through IDX, 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 identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do: We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-903-3648, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is April 6, 2025.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information: You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-903-3648 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

HMV takes your trust in us and this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read 'Roy Prestwood', with a stylized, flowing script.

Roy Prestwood, Managing Partner

333 Texas St
Ste 1525
Shreveport, LA 71101

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 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 (the “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 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
1-800-525-6285
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 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 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
877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/CPD
888-743-0023

Oregon Attorney General

1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

California Attorney General

1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General

The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

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 www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.