



Lauren Godfrey
Constangy, Brooks, Smith & Prophete, LLP
Cybersecurity & Data Privacy Team
322 North Shore Drive, Building 1B, Suite 200
Pittsburgh, PA 15212
973.462.9521
lgodfrey@constangy.com

October 10, 2023

VIA EMAIL: ldtheft@oag.state.md.us

Attorney General Brian E. Frosh
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Fax: (410) 576-6566

Re: Notification of Data Security Incident

Dear Attorney General Frosh:

Constangy, Brooks, Smith & Prophete, LLP represents Heard, McElroy, & Vestal ("HMV"), a professional services firm providing tax, accounting and other financial and consulting services located in Shreveport, Louisiana, in connection with a data security incident described in greater detail below. 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. The purpose of this letter is to notify you of the incident in accordance with Maryland's data breach notification statute, Md. Code Ann. Comm. Law §§ 14-3501 - 3508.

As noted below, a vendor error required the re-mailing of notification letters to potentially impacted individuals. Subsequent review of the deliverability of the overall notification effort confirms that the issue was rectified and that notice to impacted individuals has been successfully completed.

1. Nature of the Security Incident

On or around February 13, 2023, HMV began receiving rejection notices for tax returns filed on behalf of some of its clients' employees. HMV immediately began investigating these claims and enlisted the assistance of cybersecurity and other technical experts to investigate what happened and whether personal information in HMV's possession was accessed without authorization. The investigation determined that personal information of individuals could have been accessed or acquired.

2. Number of Affected Maryland Residents & Information Involved

The incident involved personal information for approximately 6 Maryland residents. The information involved in the incident may differ depending on the individual but may include the following for

affected Maryland residents: individuals' names, Social Security numbers, and/or financial account number.

3. **Notification to Affected Individuals**

On July 11, 2023 notification letters were sent to affected Maryland residents by USPS First Class Mail. Due to a vendor error, a subsequent notification was required and, as such, on August 22, 2023, notification letters were sent to affected Maryland residents by USPS First Class Mail.

The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers complimentary identity protection services to each individual whose Social Security numbers were affected by this event, including credit monitoring, dark web monitoring, \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. A sample notification letter, or a substantially similar version thereof, is enclosed.

4. **Measures Taken to Address the Incident**

Upon discovering this incident, in addition to taking the steps described above, HVM took steps to secure its systems and launched an investigation to learn more about what happened and what information could have been affected. HVM took immediate steps to evaluate and improve the security of its systems and will continue to evaluate additional protections that can be put into place to supplement its existing security policies and procedures as the investigation continues. HVM also reported the issue to the IRS and other relevant authorities.

HVM has established a toll-free call center through Experian to answer questions about the incident and address related concerns. Finally, HVM notified the potentially affected individuals and provided them with steps they can take to protect their personal information and is reporting the incident to nationwide consumer reporting agencies (i.e., Equifax, Experian, and Transunion).

5. **Contact Information**

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at LGodfrey@constangy.com or 973.462.9521.

Sincerely,

Lauren D. Godfrey

Lauren Godfrey
Partner, Constangy Cyber Team

LDG:mff
Encl.: Sample Notification Letter



CERTIFIED PUBLIC ACCOUNTANTS

Return Mail Processing

PO Box 589

Claysburg, PA 16625-0589

August 22, 2023

J8874-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 INDIVIDUAL

APT ABC

123 ANY STREET

ANYTOWN, ST 12345-6789



Re: Notice of Data [Extra1]

Dear Sample A. Sample:

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.

If you previously received a letter dated July 11, 2023 regarding this incident and have not yet enrolled in services, please discard the July 11, 2023 letter and contact Experian to enroll using the enrollment code provided in this letter. We apologize for any confusion that this has caused which was due to a vendor error.

What Happened: On or around February 13, 2023, HMV began receiving rejection notices for tax returns filed on behalf of some of its clients’ employees. We immediately began investigating these claims and enlisted the assistance of cybersecurity and other technical experts to investigate what happened and whether personal information in HMV’s possession was accessed without authorization. The investigation revealed that an unknown actor gained access to some client information stored on a third-party software program used by HMV. We then undertook a thorough review of the information potentially involved in the incident to identify individuals who were potentially impacted as a result of it. We recently determined that your personal information may have been involved in this incident. We then worked to obtain up to date contact information to notify you about it.

In response to the incident, we have taken immediate steps to evaluate and improve the security of 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, date of birth, Social Security number, and financial account number.

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”), the Internal Revenue Service (“IRS”), and the State Tax Administrators. We have been in contact with the IRS and State Tax Administrators to provide relevant information about this incident and will continue to provide whatever cooperation is necessary to hold the perpetrator(s) of this incident accountable.

333 Texas Street, Suite 1525
Shreveport, LA 71101

0000001



ENGAGE#

J8874-L01

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for ## months.

Please note that Identity Restoration is available to you for ## months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary ##-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** November 30, 2023 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **833-637-2101** by November 30, 2023. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR ##-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

What You Can Do. We recommend that you activate your complimentary services using the enrollment code provided below. We also recommend that you review the guidance included with this letter about how to protect your personal information.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call **833-637-2101** toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number **ENGAGE#**.

**333 Texas Street, Suite 1525
Shreveport, LA 71101**

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 'R. Prestwood', with a stylized flourish at the end.

Roy Prestwood, Managing Partner

**333 Texas Street, Suite 1525
Shreveport, LA 71101**



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 1-877322-8228, 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 105788 Atlanta, GA 30348
1-888-378-4329 www.equifax.com

Experian

P.O. Box 9532 Allen, TX 75013
1-800-831-5614 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 <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
1-877-438-4338

Maryland Attorney General

St. Paul Plaza
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
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

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>
riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General

400 S 6th 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://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.