

Jason M. Schwent
T (312) 985-5939
F (312) 517-7573
Email:jschwent@clarkhill.com

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

October 26, 2022

Attorney General Brian E. Frosh
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

We represent Renner, Williams & Mooney, LLC (“the Firm”) with respect to a data security incident involving potential exposure of certain personal identifiable information (“PII”) described in more detail below. Renner, Williams & Mooney, LLC is a full-service accounting and tax firm located in McLean, Virginia. The Firm 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 the incident.

On or about July 20, 2022, the Firm became aware of suspicious activity associated with an email account, and immediately began an investigation and hired independent cybersecurity experts to determine what occurred and whether any information was at risk. The investigation determined that there was unauthorized access to one email account, which was secured on July 20, 2022. Unfortunately, the investigation was unable to determine whether any information was accessed or acquired. Because of this, a vendor was hired to conduct an in-depth review of the email account to determine what personal information may have been stored in the account. This review was completed on September 30, 2022. From this review, it appears the information in the account during the unauthorized access may have included individuals’ names and addresses in combination with their date of birth, driver’s license number, financial account number, and Social Security number.

2. Number of residents affected.

Twelve (12) Maryland residents may have been affected and were notified of the incident. A notification letter has been sent to the potentially affected individuals on October 26, 2022 (a copy of the form notification letter is enclosed as Exhibit A).

3. Steps taken in response to the incident.

The Firm took steps to address this incident and prevent similar incidents in the future. The Firm has changed all passwords on the impacted system, enabled multi-factor authentication on all Firm email accounts and implemented additional controls. Affected individuals were offered 12 months of credit monitoring and identity protection services through Cyberscout

.

4. Contact Information.

The Firm takes the security of the information in its control very seriously and is committed to ensuring information within its control is protected. If you have any questions or need additional information, please do not hesitate to contract me at jschwent@clarkhill.com or (312) 985-5939.

Sincerely,

CLARK HILL

A handwritten signature in black ink, appearing to read 'JS', followed by a long horizontal line extending to the right.

Jason M. Schwent
Senior Counsel

JMS:bmd

cc: Lara Forde

EXHIBIT A

Renner, Williams & Mooney, LLC
P.O. Box 3923
Syracuse, NY 13220

Renner, Williams & Mooney, LLC

Certified Public Accountants

To Enroll Visit:
<https://secure.identityforce.com/benefit/rwmlc>
Enrollment Code: [REDACTED]

October 25, 2022

Notice of Data Security Incident

[REDACTED],

Renner, Williams & Mooney, LLC (the “Firm”) recently experienced a data security incident that may have impacted some of your personal information. We respect the privacy and security of your information and sincerely apologize for any concern or inconvenience this may cause you. This letter contains steps you can take to protect your information and resources we are making available to help you in doing so.

What Happened?

On or about July 20, 2022, the Firm became aware of suspicious activity associated with an email account, and immediately began an investigation and hired independent cybersecurity experts to determine what occurred and whether any information was at risk. The investigation determined that there was unauthorized access to one email account, which was secured on July 20, 2022. Unfortunately, the investigation was unable to determine whether any information was accessed or acquired. Because of this, a vendor was hired to conduct an in-depth review of the email account to determine what personal information may have been stored in the account. This review was completed on September 30, 2022, at which point we learned that some of your personal information may have been present in the account during the period of unauthorized access. While there is no indication that any of your personal information has been misused, out of an abundance of caution, we wanted to let you know about this incident and provide you with resources to help you protect yourself.

What Information Was Involved?

Information that may have been affected includes things like your name, address, Social Security number and other information provided to the Firm in order to prepare taxes.

What We Are Doing:

We want to assure you that we have taken additional steps to enhance the security of our systems. Since the incident, all passwords on the impacted system have been changed, and we have enabled multi-factor authentication on all Firm email accounts and implemented additional controls.

In addition, while we are not aware of any misuse of your information, we are offering identity theft protection services through Cyberscout at no cost to you. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday. Please call the help line 1-800-405-6108 and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described below is required.

Additionally, we are providing you with access to **Single Bureau Credit Monitoring*** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. We are also providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft. These services will be provided by Cyberscout through Identity Force, a company specializing in fraud assistance and remediation services.

To enroll in **Credit Monitoring*** services at no charge, please log on to <https://secure.identityforce.com/benefit/rwmlle> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED] In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

What You Can Do:

We encourage you to remain vigilant against incidents of identity theft by reviewing your bank account and other financial statements as well as your credit reports for suspicious activity for the next 12 to 24 months. You should also contact Cyberscout with any questions and to take advantage of the Cyberscout 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.

Additionally, if you know or suspect you are a victim of tax-related identity theft, the IRS recommends the following steps:

- Respond immediately to any IRS written notice. **The IRS will not contact you via phone.**
- If you received a Letter 5071C, 4883C or 6330C from the IRS indicating that they received a suspicious tax return with your name on it or need to verify your information, you should follow the instructions on that letter to verify your identity with the IRS. Once you verify your identity, you can advise the IRS that you did not file the suspicious tax return. Additionally, you may be asked to file a paper return for the current filing season.
- If you believe you may be a victim of tax fraud but have not received a Letter 4883C or 6330C from the IRS, you should fill out and submit IRS Form 14039, which is available at IRS.gov. We can provide you with a copy of that form and assist you with filling it out if you would like.

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

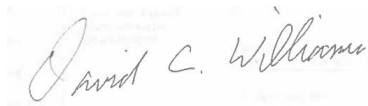
If you previously contacted the IRS and did not have a resolution, contact the IRS for specialized assistance at 1-800-908-4490. The IRS has teams available to assist. You should also visit <https://www.irs.gov/individuals/how-irs-id-theft-victim-assistance-works> for more information.

You may also want to consider contacting the IRS to obtain an E-File Pin to ensure your tax information is secure when filing next year. This information can be obtained online at the following link: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>. This online resource is the fastest way to obtain an E-File Pin, but you can also call 844-545-5640 for more information.

For More Information:

Please call 1-800-405-6108 from 8:00 am – 8:00 pm Eastern Time, Monday through Friday, for assistance or for any additional questions you may have. Your trust is our top priority and we deeply regret any inconvenience or concern this matter may cause you.

Sincerely,

A handwritten signature in cursive script that reads "David C. Williams". The signature is written in dark ink on a light-colored background.

David C. Williams

Recommended Steps to Help Protect Your Information

1. Enroll in the complimentary services with Cyberscout. You've been provided with access to the following services from Cyberscout:

Single Bureau Credit Monitoring*. You will receive alerts when there are changes to your credit data such as when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Cyberscout fraud specialist, who can help you determine if it is an indicator of identity theft.

Fraud Consultation. You have unlimited access to consultation with a Cyberscout specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration. If you become a victim of identity theft, an experienced Cyberscout licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

2. Review your credit reports. It is recommended that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

3. 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
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

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

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
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.

4. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above 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 credit files.

5. Reporting of identity theft and obtaining a police report. 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.

6. 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. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

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

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

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For 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/>.

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.