CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

MEGHAN S. FARALLY
mfarally@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

July 27, 2022

Via E-Mail (IDTheft@oag.state.md.us)
Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202

RE: Data Incident Notification

To Whom It May Concern:

We serve as counsel for Ritch, Greenberg & Hassan, P.C. ("RGH") located at 70 Platt Road, Shelton, Connecticut 06484 and write to inform you of a recent data security incident. By providing this notice, RGH does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On March 25, 2022, RGH became aware that certain client 2021 tax returns were filed using a different firm's Electronic Filing Identification Number (EFIN). Upon discovery, RGH immediately took steps to review network security, contacted law enforcement, and began an investigation with the assistance of third-party forensic specialists. On April 12, 2022, while the investigation was still ongoing, RGH provided notice to a small group of known compromised individuals. There were no Maryland residents present in the initial population.

Further investigation revealed a cyber security incident that led to the potential unauthorized access of additional client tax returns. Because there was the potential for unauthorized access to personal information contained within the tax returns, RGH compiled a list of clients potentially impacted and worked to obtain sufficient address information in order to provide notification. That process was completed on June 20, 2022. At that time, it was determined that tax information related to 15 Maryland residents was potentially subject to unauthorized access. The information contained in the tax returns subject to unauthorized access would have included first and last name, in combination with a Social Security number, bank account information, and driver's license number.

On July 27, 2022, RGH sent written notice of this incident to the potentially impacted Maryland residents pursuant to Maryland law. The notice letter included an offer of complimentary credit monitoring and identity protection services for twelve (12) months. The notice letter sent to individuals is substantially similar to the letter attached hereto as Exhibit "A."

Very truly yours,

Meghan Farally, Esq.
CIPRIANI & WERNER, P.C.

Exhibit A

Ritch
Greenberg &
Hassan, P.C.
CERTIFIED PUBLIC ACCOUNTANTS

Fouad M. Hassan, CPA
Paul R. Greenberg, CPA
John F. Worgan, CPA
Michael W. Hassan, CPA

Ritch, Greenberg & Hassan P.C.,
PO Box 466
Shelton, CT 06484

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

We are writing to inform you of an incident that may have involved your personal information as described below. We take the privacy and security of all information very seriously, and are providing you with information about the incident, our response, and steps you can take to help protect your information, should you feel it is appropriate to do so. We are also providing you with access to <<CM Length>> months of credit monitoring and identity protection services through Equifax.

On March 25, 2022, we became aware that certain Ritch, Greenberg & Hassan, P.C. client 2021 tax returns were filed using a different firm's Electronic Filing Identification Number (EFIN). Please know that the filing of fraudulent tax returns is a wide-spread issue, and is not unique to clients of Ritch, Greenberg & Hassan, P.C. Upon discovery, we immediately took steps to review our network security, contacted law enforcement, and began an investigation with the assistance of third-party forensic specialists. The investigation revealed a cyber security incident that led to the potential unauthorized access of client tax returns. Because there was the potential for unauthorized access to personal information contained within the tax returns, we then compiled a list of clients potentially impacted and worked to obtain sufficient address information in order to provide notification. That process was completed on June 20, 2022. We are now notifying potentially impacted individuals out of an abundance of caution. The personal information contained in the tax returns would have included your name, in combination with your <<Data Elements>>.

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports and account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. You may also enroll in the <<CM Length>> months of complimentary credit monitoring and identity protection services we are making available to you. Due to privacy laws, we cannot register you directly. Additional information regarding how to enroll in the complimentary services is enclosed in the attached "Steps You Can Take to Help Protect Your Information."

Should you have questions or concerns regarding this matter, please contact us at pg@rghcpa.com and copy dm@rghcpa.com. You may also call us at 203-929-6371, or write to us at 70 Platt Rd, Shelton, Connecticut 06484.

The security of information is of the utmost importance to us, and we will continue to take steps to protect information in our care.

Sincerely,

Ritch, Greenberg & Hassan P.C.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in Credit Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in a credit monitoring service for <<CM Length>> months provided by Equifax, one of the three nationwide credit reporting companies.

Your Activation Code: *<<ACTIVATION CODE>>*

Enrollment Deadline: *<<Enrollment Deadline>>*

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of ***<<ACTIVATION CODE>>*** then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header.
   Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

   You're done!
   The confirmation page shows your completed enrollment.
   Click "View My Product" to access the product features.

---

[1] WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

[2] The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

[3] Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.

[4] The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL ACTIONS TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com	**Experian** 1-888-397-3742 www.experian.com	**Equifax** 1-888-298-0045 www.equifax.com
TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000	**Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013	**Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069
TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	**Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. NW Washington, D.C. 20001; 202-727-3400; and oag@dc.gov. Ritch, Greenberg & Hassan, P.C. may be contacted at 70 Platt Road, Shelton, Connecticut 06484.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Ritch, Greenberg & Hassan, P.C. may be contacted at 70 Platt Road, Shelton, Connecticut 06484.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are <<RI Count>> Rhode Island residents impacted by this incident.