

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

August 26, 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 Jonathan S. Resnick, CPA ("Resnick") located at 1300 Bristol Street North, Suite 200, Newport Beach, California 92660 and write to inform you of a recent data security incident. By providing this notice, Resnick does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On June 16, 2022, Resnick became aware that a single client 2021 tax return was filed with fraudulent bank account information. The fraudulent filing led to state and federal tax return funds being deposited into an illegitimate bank account. Resnick subsequently became aware of one other client with a similar situation. Upon discovery, Resnick immediately took steps to review its network security, reported the incident to law enforcement, and began an investigation with the assistance of third-party forensic specialists. On July 6, 2022, while the investigation was still ongoing, Resnick provided written notice to the 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 2021 client tax returns. Because there was the potential for unauthorized access to information contained within the tax returns, Resnick then compiled a list of clients potentially impacted and worked to obtain sufficient address information in order to provide notification. On August 2, 2022, that process was completed, and it was determined that information related to 1 Maryland resident was potentially subject to unauthorized access. The information contained in the tax returns would have included first and last name, in combination with a Social Security number and bank account information.

On August 25, 2022, Resnick sent written notice of this incident to the potentially impacted Maryland resident 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

JONATHAN S. RESNICK, CPA
AN ACCOUNTANCY CORPORATION

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

RE: NOTICE OF DATA BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of an incident that may have involved your 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 12 months of credit monitoring and identity protection services through Kroll.

On June 16, 2022, we became aware that a single Jonathan S. Resnick, CPA client 2021 tax return was filed with fraudulent bank account information. The fraudulent filing led to state and federal tax return funds being deposited into an illegitimate bank account. We subsequently became aware of one other client with a similar situation. Please know that the filing of fraudulent tax returns is a widespread issue, and is not unique to our firm. Upon discovery, we immediately took steps to review our network security, reported to 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 August 2, 2022. We are now notifying potentially impacted individuals out of an abundance of caution. The information contained in the tax returns would have included your name, in combination with your <<b2b_text_1(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 activate the 12 months of complimentary credit monitoring and identity protection services we are making available to you. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Due to privacy laws, we cannot register you directly. Additional information regarding how to activate the complimentary services is enclosed in the attached "Steps You Can Take to Help Protect Your Information."

Additionally, we recommend you apply for an Identity Protection PIN (IP PIN) through the IRS. An IP PIN is a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS. It helps the IRS verify your identity when you file your electronic or paper tax return. You can apply for an IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

Should you have questions or concerns regarding this matter, please call 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding some major U.S. holidays.

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

Sincerely,

Jonathan Resnick

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring Services

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, 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 Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to help 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 Kroll 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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

You can sign up for the online identity monitoring service anytime between now and <<b2b_text_6(activation deadline)>>. Due to privacy laws, we cannot register you directly. Activating this service will not affect your credit score. You must be over age 18 with a credit file activate these services.

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 TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 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 help 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. Jonathan S. Resnick, CPA may be contacted at 1300 Bristol Street North, Suite 200, Newport Beach, CA 92660.

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. Jonathan S. Resnick, CPA may be contacted at 1300 Bristol Street North, Suite 200, Newport Beach, CA 92660.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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 [#] Rhode Island residents impacted by this incident.