

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

MEGAN FARALLY
mfarally@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

JOHN CLARK
jclark@c-wlaw.com

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

March 31, 2025

Via E-Mail (IDTheft@oag.state.md.us)

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

RE: Notice of Data Security Incident

To Whom It May Concern:

We represent Ciuni & Panichi, Inc. ("Ciuni & Panichi") located at 25201 Chagrin Blvd, Beachwood, OH 44122, and provide this notification of a recent data security incident. By providing this notice, Ciuni & Panichi does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On November 3, 2024, Ciuni & Panichi became aware of unauthorized activity in an employee email account. Upon discovery, Ciuni & Panichi began an investigation with the assistance of third-party specialists. The investigation determined an unauthorized party may have accessed certain files within the Ciuni & Panichi employee email account for a limited period of time. Thereafter, Ciuni & Panichi began a review of the potentially impacted files to determine the type of information contained therein and to whom the information related. Ciuni & Panichi completed this review on January 21, 2025, and determined information related to clients it provides accounting services to was impacted. Ciuni & Panichi notified impacted client data owners on February 14, 2025 and offered to notify impacted individuals on their behalf.

The review of the potentially impacted client files determined 495 Maryland residents were potentially impacted by this incident. The types of information potentially impacted include individual's name in combination with one or more of the following elements: Date of Birth and Social Security Number. Ciuni & Panichi began sending individual notification letters on behalf of client data owners on March 27, 2025, via First Class mail. This mailing included the residents of Maryland believed to be impacted.

In response to this incident, Ciuni & Panichi conducted a full forensic investigation, changed passwords, updated its data security policies, improved its data security measures, and notified impacted individuals. A template copy of the individual notification letter sent to individuals on behalf of data owners is attached hereto as *Exhibit A*.

Thank you for your attention to this matter. Please contact me should you have any questions.

Very truly yours,

By: 

Meghan Farally, Esq.

Cipriani & Werner, P.C.

Exhibit A



P.O. Box 989728
West Sacramento, CA 95798-9728

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

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

March 27, 2025

<<Header>>

Dear <<First Name>> <<Last Name>>:

Ciuni & Panichi, Inc. (“Ciuni & Panichi”) writes to you on behalf of <<Full Data Owner Name>> regarding a recent event that may have impacted certain information related to you. Ciuni & Panichi provides accounting services to <<Full Data Owner Name>> and was in possession of your information due to this business relationship. This letter includes information about the event, our response, and resources we are making available to you.

What Happened? On November 3, 2024, Ciuni & Panichi became aware of unauthorized activity in an employee email account. Upon discovery, we took steps to secure the affected account and engaged a third-party team of forensic specialists to investigate the incident. On January 21, 2025, following a thorough review, we confirmed that a limited amount of information may have been accessed by an unauthorized third party in connection with this incident. At this time, there is no indication that any personal information has been or will be fraudulently misused. However, we are providing this notification to you out of an abundance of caution and so that you may take steps to help safeguard your information.

What Information Was Involved? The information potentially impacted includes your name in combination with one or more of the following data elements: <<Data Elements>>.

What We Are Doing. In response to this event, Ciuni & Panichi reset passwords, secured all accounts, and conducted a full investigation into the incident. Additionally, in an abundance of caution, Ciuni & Panichi is offering you access to <<12/24>> months of credit monitoring and identity protection services at no cost to you. Due to privacy laws, Ciuni & Panichi cannot activate these services for you directly. Additional information regarding how to activate the complimentary credit monitoring service is enclosed.

What You Can Do. Ciuni & Panichi recommends that you remain vigilant against incidents of fraud and identity theft by reviewing your credit reports/account statements and explanation of benefits forms 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. Additionally, you can enroll to receive the complimentary credit monitoring service we are making available to you. You can also review the enclosed “Steps You Can Take to Help Protect Your Information” for additional resources.

For More Information. We understand you may have questions about this incident. You may call 1-877-332-0172 Monday through Friday from 9am to 9pm Eastern Time, excluding holidays, or write to us at 25201 Chagrin Blvd, Beachwood, OH 44122.

Ciuni & Panichi sincerely regrets any concern this incident may cause you. The privacy and security of your information is important to us, and we will continue to take steps to protect information in our care.

Sincerely,

Ciuni & Panichi, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring / Identity Protection

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you. Please note the deadline to enroll is June 27, 2025.

3. Telephone. Contact IDX at 1-877-332-0172 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms 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 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 Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

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: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. 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 https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 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 Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-442-9828, and <https://oag.dc.gov/consumer-protection>.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 33 Rhode Island residents impacted by this incident.