



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

James Cope
Office: (267) 930-4766
Fax: (267) 930-4771
Email: JCOPE@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

October 24, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Chimienti & Associates (“Chimienti”) located at 3130 W Main St suite 106, Visalia, CA 93291, and we are writing to notify your office of a matter that may affect the security of certain information relating to nine (9) Maryland residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Chimienti does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On March 22, 2024, Chimienti identified suspicious activity occurring within a single internal email account. In response, Chimienti conducted an investigation to understand the nature and scope of this event and determined that an unauthorized actor viewed and/or copied data from the email account between March 22 and March 26, 2024. With the assistance of third-party review specialists, Chimienti conducted a thorough, in-depth review of the email account to determine what information was impacted and to whom the information relates. The comprehensive review was completed on September 11, 2024. Chimienti then conducted a thorough analysis of the results of this review internally to confirm address information for the individuals identified and on October 11, 2024, confirmed information related to nine (9) Maryland residents.

The information that could have been subject to unauthorized access includes name and Social Security number.

Notice to Maryland Residents

On or about October 24, 2024, Chimienti began providing written notice of this event to nine (9) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon becoming aware of this event, Chimienti investigated and responded to it, assessed the security of its network, and notified potentially affected individuals. Further, Chimienti regularly reviews and enhances its already robust policies and procedures related to data privacy to reduce the likelihood of a similar event reoccurring in the future. As an added precaution, Chimienti is offering credit and identity monitoring through CyEx for twelve (12) months, at no cost to these individuals.

Additionally, Chimienti is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Chimienti is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Chimienti is also providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the event, please contact us at (267) 930-4766.

Very truly yours,

James Cope of
MULLEN COUGHLIN LLC

JC1/bxn
Enclosure

EXHIBIT A



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

<<Var Data 1 - NOTICE OF DATA BREACH>>

Dear <<Full Name>>:

Chimienti & Associates ("Chimienti") writes to notify you about an event that may affect certain information related to you. This letter provides you with details about what occurred, our response, and the resources available to assist you with safeguarding your information, should you feel it appropriate to do so.

What Happened? On March 22, 2024, Chimienti identified suspicious activity occurring within a single internal email account. In response, we conducted an investigation to understand the nature and scope of this event and determined that an unauthorized actor viewed and/or copied data from the email account between March 22 and March 26, 2024. With the assistance of third-party review specialists, we conducted a thorough, in-depth review of the email account to determine what information was impacted and to whom the information relates. Upon completion of the third-party review, we reviewed the results internally to confirm contact information for the individuals identified, and on October 11, 2024, confirmed that information related to you was in the relevant email account at the time of the event.

What Information Was Involved? The review of the impacted data identified the following information related to you: name and <<data elements>>.

What We Are Doing. We take the confidentiality of personal information in our care seriously. Upon becoming aware of this event, we investigated and responded to it, assessed the security of our email tenant, and notified potentially affected individuals. As part of our ongoing commitment to the privacy and security of information in our care, we regularly review and enhance our already robust policies and procedures related to data privacy to reduce the likelihood of a similar event reoccurring in the future.

As an added precaution, we are also offering credit and identity monitoring through CyEx for <<12 months/24 months>>, at no cost to you. If you wish to activate these services, please follow the instructions included in the attached *Steps You Can Take to Help Protect Your Personal Information*. Please note, due to privacy restrictions, we are unable to enroll you in these services on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You should report any suspicious charges on your credit or debit card to the bank that issued the card or to the card company, as appropriate. You may also review the *Steps You Can Take to Help Your Protect Personal Information* section of this letter, which contains additional information and resources, including information to enroll in the complimentary credit monitoring services offered to you.

For More Information. If you have any questions about this matter, please contact our dedicated assistance line at 1-855-277-8328, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time, except holidays. You may also write to us at Chimienti & Associates, Attn: Janet Moore, Director of Client and Account Services, 3130 W. Main Street Suite 106 Visalia, CA 93291.

Sincerely,

Chimienti & Associates

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in Monitoring Services

Identity Defense Complete

Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- \$1 Million Identity Theft Insurance**

Enrollment Instructions

To enroll in Identity Defense, visit **{{URL}}**

1. **Enter your unique Activation Code:** <<Activation Code>>
Enter your Activation Code and click 'Redeem Code'.
2. **Create Your Account**
Enter your email address, create your password, and click 'Create Account'.
3. **Register**
Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. **Complete Activation**
Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Enrollment Deadline>>. After <<Enrollment Deadline>>, the enrollment process will close, and your Identity Defense code will no longer be active. **If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.**

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 1-866-622-9303.

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.

**Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage,

or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

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

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

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert P.O. Box 105069, Atlanta, GA 30348	Experian Fraud Alert P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze P.O. Box 105788, Atlanta, GA 30348	Experian Credit Freeze P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. 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; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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 Avenue NW, Washington, DC 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; and <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.