



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Gregory Lederman
Office: (267) 930-4637
Fax: (267) 930-4771
Email: glederman@mullen.law

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

March 27, 2023

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

Dear Sir or Madam:

We represent Tenney & Company CPA's ("Tenney") located at 1528 Starr Drive, Suite A, Yuba City, CA 95993, and are writing to notify your Office of an incident that may affect the security of certain information relating to one (1) Maryland resident. By providing this notice, Tenney 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 or about May 19, 2022, Tenney identified suspicious activity relating to certain systems within its computer network and immediately launched an investigation to determine the nature and scope of the activity. The investigation determined that an unknown actor gained access to certain Tenney systems between April 13, 2022 and May 19, 2022. In an abundance of caution, Tenney conducted a thorough review of the impacted systems in order to identify individuals whose information was present on the impacted systems at the time of the activity and to whom this information belonged. On or about January 12, 2023, Tenney's review of the impacted systems was completed and determined that the following types of information related to potentially impacted individuals includes name, address, Social Security number, tax identification number, and financial account information..

Notice to Maryland Resident

On or about March 27, 2023, Tenney provided written notice of this incident to one (1) Maryland resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Notification to impacted clients and individuals is ongoing, and Tenney may supplement this notification if it is determined that a significant amount of additional Maryland resident will receive notice.

Other Steps Taken and To Be Taken

Upon discovering the event, Tenney moved quickly to investigate and respond to the incident, assess the security of Tenney systems, and identify potentially affected individuals. Further, Tenney notified federal law enforcement regarding the event. Tenney is also working to implement additional safeguards and training to its employees. Tenney is providing access to complimentary credit monitoring services for one year, through Equifax, to individuals whose information was potentially affected by this incident.

Additionally, Tenney is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Tenney is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4637.

Very truly yours,



Gregory Lederman of
MULLEN COUGHLIN LLC

GCL/nad
Enclosure

EXHIBIT A



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

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

<<Date>>

NOTICE OF DATA BREACH

Dear <<Name 1>>:

Tenney & Company CPA's ("Tenney") is writing to inform you of a recent event that may impact some of your information. We received your information in connection with account/tax/business financial services provided to you. Although there is no indication that your information has been misused in relation to this event, we are providing you with information about the event, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened? In May 2022, Tenney identified suspicious activity relating to certain systems within its computer network and immediately launched an investigation to determine the nature and scope of the activity. The investigation determined that an unknown actor gained access to certain Tenney systems between April 13, 2022, and May 19, 2022. In an abundance of caution, Tenney conducted a thorough review of the impacted systems in order to identify individuals whose information was present on the impacted systems at the time of the activity.

What Information Was Involved? Tenney's review of the impacted systems was recently completed and we are notifying you now because the investigation determined that the following types of information related to you may have been present on the impacted systems during this incident: name, address, Social Security number, and/or financial account information associated with your tax documentation. Tenney is not aware of any actual or attempted misuse of information as a result of this incident.

What We Are Doing. The security, confidentiality, and privacy of information in our care is important to us and we have strict security measures in place to protect this information. Upon learning of this event, we worked quickly to secure our systems and further enhance our network security by implementing additional safeguards and are reviewing our existing policies and procedures regarding cyber security. We reported the event to federal law enforcement and are notifying appropriate state regulators.

Although we are unaware of any misuse of your information as a result of this incident, as an additional precaution, Tenney is offering you access to twelve (12) months of complimentary credit monitoring and identity restoration services through Equifax. Details of this offer and instructions on how to activate these services are enclosed with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and free credit reports for suspicious activity and to detect errors. Additional information and resources are contained in the enclosed *Steps You Can Take to Help Protect Your Information*. You may also enroll in the complementary credit monitoring services available to you.

For More Information. If you have additional questions or concerns, you may call our toll-free dedicated assistance line at 888-351-3934. This toll-free line is available Monday – Friday (except U.S. holidays) from 6:00 am PT and 6:00pm PT. You may also write to Tenney at 1528 Starr Drive, Suite A, Yuba City, CA 95993.

We sincerely regret any inconvenience this event may cause.

Sincerely,

Jerome Tenney
Owner
<http://www.tenney-cpa.com/>

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring



<FIRST NAME> <LAST NAME>

Enter your Activation Code: <ACTIVATION CODE>
Enrollment Deadline: <DEADLINE MMMM DD, YYYY>

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ 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 alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- 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 theft⁴

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.

¹WebScan 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.

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

³Locking 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.

⁴The 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.

File Your Tax Return

While we are unaware of an actual or attempted misuse of this information, we encourage you to file your tax return as soon as possible, if you have not already done so. You can also contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You should also look to the information made available by the tax authority for your state of residence and any other state where you file a tax return. For a list of websites for each US state's tax authority, visit <http://www.taxadmin.org/state-tax-agencies>.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report 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 security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place a credit freeze, 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
888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	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 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 and your 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; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

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.