



June 2, 2023

Via email: ldtheft@oag.state.md.us

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Dear Anthony:

We are informing you of a recent data security incident (“Matter”) that concerned the personal information (collectively the “Information”) of individuals associated with our client, Michael S Coffman CPA (“Coffman”). There is currently no evidence to indicate actual misuse of the Information. However, out of an abundance of caution and in compliance with state law, we are reporting this Matter.

What Happened?

On March 16, 2023, Coffman’s tax software provider informed Coffman of unusual activity on Coffman’s firm account. Coffman’s provider had claimed to have similar unusual activity with other tax preparation firms as well indicating a “known server” attempting to electronically file tax returns from another location. At the advice of my cyber insurance company, Coffman engaged high level data incident response professionals and they investigated the Matter. The IRS was notified and electronic filing ceased immediately. The incident response investigation concluded on May 17, 2023, and it was determined that Information was impacted. At this time, Coffman notified the preparers of the incident and discussed my plans to communicate this to them via the notice letter. There was no evidence of actual misuse of the Information. Therefore, as required under state breach notification laws, Coffman will provide notice to the affected individuals. The total number of affected individuals was 55. Of the total, 3 individuals are Maryland residents. Notice to affected individuals will be completed on June 2, 2023.

What Information was Involved?

The Information that was impacted includes:

- First and Last Name
- Social Security number (“SSN”)

What mitigation steps were taken?

As returns are rejected by the IRS, Coffman's procedure was to inform the client of the reject and file paper returns. Data security professionals have implemented additional security measures and took a number of risk mitigation steps.

Coffman also secured credit monitoring services to provide identity and credit monitoring services for 12 months (or longer if required by each applicable state notification law) to the Individuals who had their SSN impacted along with their first and last names.

Please let us know if you have any additional questions.

Very truly yours,

The Beckage Firm

By: 

Shawn M.B. Ford, LL.M., Esq.
Member, IR Group Lead

E – sford@thebeckagefirm.com

T – 905-409-1385

<Return Name>
c/o Cyberscout
<Return Address>
<City> <State> <Zip>

<FirstName> <LastName>
<Address1>
<Address2>
<City><State><Zip>

June xx, 2023

Dear <First Name> <Last Name>,

I am writing to inform you of a recent data security incident (“Matter”) that may concern some of your personal information (collectively the “Information”). While I currently have no evidence of actual misuse of your Information, I am sharing what I know about the Matter, my response to it, and steps you can take to help protect your Information.

What Happened?

On March 16, 2023, my tax software provider informed me of unusual activity on my firm’s account. My provider had claimed to have similar unusual activity with other tax preparation firms as well indicating a “known server” attempting to electronically file tax returns from another location. At the advice of my cyber insurance company, I engaged high level data incident response professionals and they investigated the Matter. The IRS was notified and electronic filing ceased immediately. The incident response investigation concluded on May 17, 2023, and it was determined that your Information was impacted. At this time, I notified the preparers of the incident and discussed my plans to communicate this to you via this letter. There was no evidence of actual misuse of your Information, however, out of an abundance of caution, I am notifying you because your information was impacted.

What Information was Involved?

The Information that may be impacted includes:

- First and Last Name
- Social Security number (Social Insurance Number)

What Are We Doing?

As returns are rejected by the IRS, our procedure is to inform the client of the reject and file paper returns. Some of you may have already been contacted by the IRS to provide additional security information to process your return. Data security professionals have implemented additional security measures and took a number of risk mitigation steps. I am proud of the quick

response by my software provider and the incident response team.

I am providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to **<unique URL>** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<unique code>**

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What Can You Do?

I encourage you to remain vigilant in reviewing your Information, such as reviewing your account statements, and monitor credit reports for any suspicious activity. I encourage you to enroll to receive identity and credit monitoring services. Please note that you must enroll directly. I am unable to enroll in these services for you.

For More Information.

You may still feel the need to speak with me regarding this Matter. If so, please call Michael S. Coffman at 217-875-5080 Ext 108 from 9:00 a.m. to 5:00 p.m. Central Time, Monday through Friday.

I apologize for any inconvenience this may have caused.

Sincerely,

A handwritten signature in cursive script that reads "Michael Coffman".

Michael S Coffman CPA
3110 N Kandy Ln
Decatur, IL 62526
mike@coffmancpas.com

Steps You Can Take To Protect Your Information

Monitor Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze	Equifax P.O. Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifax.com/personal/credit-report-services
---	--	---

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your 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 agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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 Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; or www.oag.state.md.us.