

Buffalo
New York
Chicago
Washington D.C.



www.octillolaw.com

June 4, 2024

VIA EMAIL

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

Dear Sir or Madam:

On behalf of Anderson, Davis & Associates, CPA, PA (“Anderson Davis”), and pursuant to the Personal Information Protection Act (“PIPA”), Md. Code Ann. Comm. Law § 14-3504, this letter provides notice of a recent data security incident. By providing this notice, Anderson Davis does not waive any rights or defenses, including regarding the applicability of Maryland law or personal jurisdiction.

On or about March 19, 2024, Anderson Davis first learned that one of its clients failed to receive their tax refund after Anderson Davis had filed this clients’ return. Out of an abundance of caution, Anderson Davis commenced an investigation and determined that this situation was the result of suspicious activity on a single laptop within its system (the “Incident”). Anderson Davis immediately took steps to contain and remediate any activity related to the Incident, including quarantining and disconnecting the laptop at issue, proactively changing passwords, and implementing endpoint detection and response software to its systems. At the same time, Anderson Davis notified the Internal Revenue Service, Federal Bureau of Investigation, and state tax authorities and reviewed its systems to identify any other affected clients.

Anderson Davis’s investigation determined that unauthorized actors leveraged their access to the laptop to fraudulently redirect tax refunds in an attempt to collect improper funds from the Federal Government. As a result, Anderson Davis notified the affected individuals that it identified in its review and resolved any tax filing or refund issues with the affected individuals and tax authorities.

Anderson Davis has identified sixty-nine (69) residents of Maryland who may have been affected by the security Incident. The information potentially subject to the Incident includes information typically included within a tax file including: name, social security number, tax identification number, and driver’s license number.

At this time, Anderson Davis has taken steps, on top of its already robust security protections, to further protect its systems, including implementing multi-factor authentication and deploying endpoint detection and response software. Anderson Davis also implemented additional security protocols

Office of the Attorney General

June 4, 2024

Page 2

designed to protect its network, email environment, and systems, and is currently assessing the entirety of its information security program.

Attached for your convenience is a copy of the template notification that is being sent to the impacted Maryland residents via regular mail today. Included in these notifications is a complimentary offer for 12 months of cost-free credit and/or identity monitoring.

Please feel free to contact me with any questions at (716) 898-2102 or pmcnally@octillolaw.com.

Sincerely,

OCTILLO



Patrick D. McNally, Esq.

Certified Information Privacy Professional, United States (CIPP/US)

Encl.



Return Mail Processing
PO Box 999
Suwanee, GA 30024

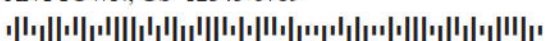
1 191 *****SINGLP

SAMPLE A. SAMPLE - L01

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



June 4, 2024

Dear Sample A. Sample,

As a valued client of Anderson, Davis & Associates, CPA, PA (“Anderson Davis” or “we”) we are writing to inform you that we recently experienced a data incident (“Incident”) which involved your personal information (“Information”). This letter provides you with information about this Incident, our response, and information on where to direct your questions. Additionally, as a precaution we have provided steps you can take to protect your Information.

What Happened?

As you know, in late March 2024, we first learned that a client failed to receive their tax refund after we filed the client’s return. Out of an abundance of caution, we commenced an investigation and determined that this situation was the result of suspicious activity on a single laptop within our system. Upon this discovery, we immediately took steps to contain and remediate any activity related to the Incident, including quarantining and disconnecting the laptop at issue, proactively changing passwords, and implementing endpoint detection and response software to our systems. At the same time, we notified the Internal Revenue Service, Federal Bureau of Investigation, and state tax authorities, and reviewed our systems to identify any other affected clients. Our investigation determined that unauthorized actors leveraged their access to the laptop to fraudulently redirect tax refunds in an attempt to collect improper funds from the Federal Government. As a result, we notified the affected individuals we identified in our review and resolved any tax filing or refund issues with the affected individuals and tax authorities.

To fully understand this situation, we also engaged leading data security and privacy professionals to assist our investigation and response. We analyzed the records from our investigation to confirm the identities of the individuals potentially affected by this Incident and notified them. Our investigation concluded that your Information was present in the affected systems at the time of the Incident.

What Information Was Involved?

We have determined that unauthorized actors may have accessed information included within your tax file, potentially including your name, date of birth, social security number, tax identification number, bank account and routing numbers, and driver’s license number. Except for the unauthorized actors’ attempts to collect improper funds from the Federal Government and/or State governments, our investigation did not identify any other misuse of information related to the Incident.

Anderson, Davis & Associates, Certified Public Accountants, PA
Suite 204 Crain Professional • 1406B South Crain Highway • Glen Burnie, Maryland 21061
Phone: 410.766.2645 • Fax: 410.766.3110
www.andersondaviscpa.com

What We Are Doing.

Upon becoming aware of the Incident, we immediately implemented additional technical safeguards on top of our significant, existing protections, including implementing multi-factor authentication and deploying endpoint detection and response software. We worked with leading data security and privacy professionals to aid in our response and reported this Incident to relevant government agencies and federal law enforcement. We also implemented additional security protocols designed to protect our network, email environment, and systems, and are currently assessing the entirety of our information security program.

To alleviate concerns and help protect your information, we are also offering a complimentary 12-month membership in Experian IdentityWorks. While identity restoration assistance is immediately available to you, we encourage you to activate the complimentary 12-month membership to Experian IdentityWorks. This product will provide you with superior identity detection and identity theft resolution. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by September 30, 2024**. (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [REDACTED], Monday through Friday from 8 am – 8 pm CST (excluding major U.S. holidays), by September 30, 2024. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

What Can You Do?

In addition to enrolling in Experian IdentityWorks, experts encourage simple steps for protecting your personal information, including changing your passwords regularly, monitoring your personal accounts closely, reporting suspicious activity to your financial institutions, and never sharing your personal information with unknown or untrusted sources. Please also review the enclosed "Additional Resources" section included with this letter, which describes additional steps you can take to help protect your Information.

For More Information.

We take this Incident and the security of information in our care seriously. If you have further questions or concerns, please call Michael Davis at 410-766-2645, Monday through Friday from 9 am – 5 pm Eastern (excluding some U.S. national holidays).

Sincerely,

ANDERSON, DAVIS & ASSOCIATES, CPA, PA

Michael Davis

Michael C. Davis, CPA
Partner

Encl.

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland Residents: You may obtain information about steps you can take to avoid identity theft from the Federal Trade Commission (contact information above) and the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1-888-743-0023.

For Pennsylvania Residents: You may contact the Pennsylvania Office of the Attorney General, Bureau of Consumer Protection, 15th Floor, Strawberry Square, Harrisburg, PA 17120, www.attorneygeneral.gov, 1-800-441-2555.

Additional Details Regarding Your 12-Month Experian IdentityWorks Membership: A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

Experian credit report at signup: See what information is associated with your credit file. Daily credit reports are available for online members only.*

- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.