Colin D. Scanlon
Office: (267) 930-4259
Fax: (267) 930-4771
Email: cscanlon@mullen.law

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

October 4, 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 Allied CPAs, P.C. ("Allied") located at 90 Linden Oaks, Suite 100, Rochester, NY 14625, and are writing to notify your office of an incident that may affect the security of certain personal information relating to forty-five (45) Maryland residents. By providing this notice, Allied 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 June 22, 2024, Allied was alerted to suspicious activity within its network. Allied immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. The investigation determined that an unauthorized actor gained access to the email account of an Allied employee and its tax preparation software. Thereafter, Allied undertook a comprehensive review of the contents of the data determined to be at risk as a result to assess what information was contained therein and to whom it related. On August 26, 2024, Allied finalized this review and determined that information related to certain Maryland residents could have been affected. The information that could have been subject to unauthorized access includes name, Social Security number, driver's license number, and financial account information.

Notice to Maryland Residents

On October 4, 2024, Allied provided written notice of this incident to forty-five (45) 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 discovering the event, Allied moved quickly to investigate, assess the security of its systems, notify law enforcement, and identify potentially affected individuals. Allied is providing individuals whose personal information was potentially affected by this incident with access to credit monitoring services for one (1) year through CyberScout at no cost to the individuals.

Additionally, Allied is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Allied 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.

Additionally, Allied is providing written notice of this incident to relevant state regulators 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 data security event, please contact us at (267) 930-4259.

Very truly yours,

Colin D. Scanlon of
MULLEN COUGHLIN LLC

CDS/jrm
Enclosure

EXHIBIT A

Allied CPAs, PC
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
DB09423

2_0000180

0000180

allied
CPAs, PC

October 4, 2024

NOTICE OF SECURITY INCIDENT

Dear :

Allied CPAs, P.C. ("Allied") is writing to notify you of an incident that may have impacted your information. This letter provides details of the incident, our response, and steps you may take to help protect your information should you feel it's appropriate to do so. Notably, Allied's sister companies, Allied Payroll Services and Allied Financial Services, Inc., were not impacted by this event. Additionally, if Allied provided tax preparation services to your business, please note that your business information was not impacted in this event.

What Happened? On June 22, 2024, Allied was alerted to suspicious activity within its network. Allied immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. The investigation determined that an unauthorized actor gained access to the email account of an Allied employee and its tax preparation software. Thereafter, Allied undertook a comprehensive review of the contents of the data determined to be at risk as a result to assess what information was contained therein and to whom it related. On August 26, 2024, Allied finalized this review and determined that information related to you could be affected.

What Information Was Involved? The information potentially impacted by this incident includes your: name, Social Security number, date of birth, and financial account information.

What We Are Doing. Allied takes the confidentiality, privacy, and security of information in its care very seriously. Upon discovering this incident, Allied conducted a diligent investigation to confirm the full nature and scope, took prompt steps to ensure security of its network environment, and conducted a comprehensive review of the information potentially affected. Allied also notified law enforcement and enhanced its existing security protocols.

In response to the incident, Allied is providing you with access to complimentary credit monitoring 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, a TransUnion company specializing in fraud assistance and remediation services. Information regarding these services and instructions on how to enroll can be found in the enclosed *Steps You Can Take to Help Protect Your Personal Information*. Please note that you must complete the enrollment process yourself as we are not permitted to enroll you in these services.

What You Can Do. Allied encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. Allied encourages you to enroll in the complementary services being offered.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-833-566-7816 and supply the fraud specialist with your unique code provided in the enclosure. You may also write to Allied CPAs, P.C. at 90 Linden Oaks, Suite 100, Rochester, NY 14625.

Sincerely,

Allied CPAs, P.C.

Steps You Can Take To Help Protect Your Personal Information

Enroll in Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to **https://www.mytrueidentity.com** and follow the instructions provided. When prompted please provide the following unique code to receive services:

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.

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 30348-5069	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

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, D.C. 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

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 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 Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 13 Rhode Island residents that may be impacted by this event.