

MARIO AYOUB
mayoub@bsk.com
P: 716.416.7023
F: 716.416.7001

October 9, 2024

VIA ELECTRONIC MAIL (IDTHEFT@OAG.STATE.MD.US)

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

Re: *Notice of Security Incident*

To Whom It May Concern:

We represent Fitzgerald, DePietro & Wojnas CPAs, P.C ("FDW") and write to provide notice of a security incident (the "Incident") that may have impacted its clients' personal information.

On June 19, 2024, FDW discovered that a threat actor had gained access to its network and deployed malicious code to encrypt and retrieve certain files. Despite taking prompt remedial action, which included severing the threat actor's access to its network, the threat actor was able to access and download tax documents and other records containing personal information. On or about August 26, 2024, FDW confirmed that personal information associated with 39 Maryland residents may have been impacted.

The following information may have been involved: (1) full names; (2) demographic information such as DOB and marital status; (3) Social Security numbers; (4) contact information such as mailing addresses and telephone numbers; and (5) financial information such as tax documents and financial account information.

As soon as FDW learned of this Incident, it took affirmative steps to sever the threat actor's access, reset IT passwords, and harden its network. With the help of hired IT professionals, FDW was able to restore functionality of its computer systems, restore files from backups, and deploy software to ensure that the threat actor was out of FDW's systems.

FDW also engaged cybersecurity counsel and a forensics firm to guide it through the Incident response process. To mitigate any potential impact on those affected, FDW is offering identity theft protection services through IDX. The identity protection services include: up to 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services.

Office of the Attorney General
October 9, 2024
Page 2

The attached notification letters were mailed to impacted individuals on September 26, 2024. FDW apologizes for any inconvenience this incident may have caused and remains steadfast in its commitment to protect personal information.

Very truly yours,

BOND, SCHOENECK & KING, PLLC

A handwritten signature in dark ink, appearing to read "Mario Ayoub", written over a light gray rectangular background.

Mario Ayoub

(Attachment)



PO Box 480149
Niles, IL 60714

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://response.idx.us/fdwcpa>

September 26, 2024

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a recent security incident (the “Incident”) at Fitzgerald, DePietro & Wojnas CPAs, P.C. (“FDW” or “we”) that may have impacted your personal information. We take the protection of your personal information very seriously and want to provide you with details about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened

On June 19, 2024, we discovered that a threat actor had gained access to FDW’s network and deployed malicious code to encrypt and retrieve our files. Despite taking prompt remedial action, which included severing the threat actor’s access to our networks, the threat actor was able to access and download tax documents and other records containing the personal information of impacted individuals. On or about August 26, 2024, we have determined that your personal information was involved in this Incident.

What Information Was Involved

The following information may have been involved: (1) your full name; (2) demographic information such as your DOB and marital status; (3) Social Security number; (4) contact information such as your mailing address and telephone number; and (5) financial information such as your tax documents and financial account information.

What We Are Doing

As soon as we learned of this Incident, we took affirmative steps to sever the threat actor’s access, reset IT passwords, and harden our network. With the help of IT professionals, we were able to get our computer system functional, restore our files from backups, and deploy software to ensure that the threat actor was out of our system. We also engaged cybersecurity counsel and a forensics firm to guide us through the Incident response process.

In addition, we are offering identity theft protection services through IDX, A ZeroFox Company, a data breach and recovery services expert. IDX identity protection services include: <<Membership Offering Length>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling (877) 225-2095, going to <https://response.idx.us/fdwcpa>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is December 26, 2024.

We encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call (877) 225-2095 or go to <https://response.idx.us/fdwcpa> for assistance or for any additional questions you may have.

We apologize for any inconvenience this Incident may have caused.

Sincerely,

Fitzgerald, DePietro & Wojnas CPAs, P.C.

291 Genesee St
Utica, New York, 13501

(Enclosure)



Recommended Steps to help Protect your Information

1. Website and Enrollment. Scan the QR image or go to <https://response.idx.us/fdwcpa> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at (877) 225-2095 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General. You have the right to obtain a police report.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You 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. You can review your 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 Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <http://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.