



Jackson Lewis P.C.
10701 Parkridge Blvd.
Suite 300
DC Region, VA 20191
(703) 483-8300 Main
(703) 483-8301 Fax
www.jacksonlewis.com

Jackson Biesecker
Direct: (216) 750-4303
Jackson.Biesecker@jacksonlewis.com

VIA EMAIL (idtheft@oag.state.md.us)

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

Re: Data Incident Notification¹

September 27, 2024

Dear Sir or Madam:

Pursuant to Md. Code Com. Law § 14-3504, we are writing on behalf of our client, Edwards CPA Group P.C. (“Edwards CPA”), to notify your office of a data security incident affecting one (1) Maryland resident. Edwards CPA is located at 51 Park St, Northfield, NH 03276.

On or about June 27, 2024, Edwards CPA discovered its systems had been subject to unauthorized access by a bad actor from approximately June 2-3, 2024 (the “Incident”). We note that the Incident did not involve a ransomware attack. With assistance from third-party experts, Edwards CPA took immediate steps to secure its systems and investigate the nature and scope of the Incident.

Through its investigation, Edwards CPA learned that affected systems stored personally identifiable information (“PII”) for some individuals, including: name, address, Social Security number, driver’s license number or state ID, and/or passport number. The investigation did not observe any evidence that personal information was removed from our environment.

Out of an abundance of caution, and in accordance with applicable law, Edwards CPA will provide notice to the affected Maryland resident so that they can take steps to minimize the risk that their information will be misused. Edwards CPA will begin sending these notices in the coming days. A sample notice letter is enclosed. Additionally, Edwards CPA has arranged for notice recipients to enroll in free credit monitoring and related services for 12 months, including identity theft insurance up to \$1,000,000 as well as identity recovery and restoration services.

¹ Please note that by providing this letter Edwards CPA Group P.C. is not agreeing to the jurisdiction of the State of Maryland, nor waiving its right to challenge jurisdiction in any subsequent actions.

As set forth in the enclosed letter, Edwards CPA has taken steps to protect the security of the personal information of all individuals. Edwards CPA endeavors to protect the privacy and security of sensitive information and has worked diligently to determine how this incident happened and are taking appropriate measures to prevent a similar situation in the future. Since the Incident, Edwards CPA has: migrated to a cloud-based tax preparation solution, reset all passwords, and changed to a new cybersecurity and IT managed services provider with 24/7/365 SOC monitoring.

If you require any additional information on this matter, please call me.

Sincerely,

JACKSON LEWIS, P.C.

/s/ Jackson E. Biesecker

Jackson E. Biesecker

Enclosure



Edwards CPA Group P.C.
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>> or <<IMB>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

September 27, 2024

Incident Notice

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

This letter is from Edwards CPA Group P.C. (“Edwards CPA”). We are sorry to tell you about a data security incident that may have involved some of your personal information. Edwards CPA takes the protection of your information seriously, and we regret any inconvenience this may cause.

What Happened

On or about June 27, 2024, we identified that some of our systems were subject to unauthorized access from approximately June 2nd to 3rd, 2024 (the “Incident”). After discovering the Incident, we immediately commenced an investigation with assistance from third party cybersecurity experts for the purpose of determining its scope.

You are receiving this letter because your personal information was stored on systems that were subject to unauthorized access. The investigation did not observe any evidence that your personal information was removed from our environment. We have also not found any evidence that any of your information was misused.

What Information Was Involved

The information stored on impacted systems may have included your name, address, birthdate, and/or Social Security Number.

What We Are Doing

Out of an abundance of caution, we are providing this notice to you so that you can take steps to minimize the risk that your information could be misused. The attached sheet describes steps you can take to protect your identity, credit, and personal information.

As an added precaution, we are offering identify theft protection services through IDX. IDX identity protection services include 12 months of credit monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this specialized protection, IDX can help you resolve issues if your identity is compromised.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4170 or going to <https://app.idx.us/account-creation/protect> and using the enrollment code [code]. IDX

representatives are available Monday through Friday from 9:00 am to 9:00 pm Eastern Time. Please note that the deadline to enroll is December 27, 2024.

Edwards CPA treats all sensitive information in a confidential manner and is proactive in the careful handling of such information. Since the Incident, we have taken a number of steps to further secure our systems. Specifically, we have: migrated to a cloud-based tax preparation solution, reset all passwords, and changed to a new cybersecurity and IT managed services provider with 24/7/365 SOC monitoring.

What You Can Do

In addition to enrolling in the credit monitoring services discussed above, the attached sheet describes steps you can take to protect your identity, credit, and personal information.

For More Information

Please call 1-800-939-4170 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have. 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.

We sincerely apologize for this situation and any concern or inconvenience it may cause you.

Sincerely,

A handwritten signature in black ink that reads "Kim Edwards". The signature is written in a cursive, flowing style.

Kim Edwards
Edwards CPA Group P.C.

PLEASE SEE NEXT PAGE FOR ADDITIONAL INFORMATION

What You Should Do To Protect Your Personal Information

We recommend you remain vigilant and consider taking the following steps to protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:
 - Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
 - You can also receive information from these agencies about avoiding identity theft, such as by placing a “security freeze” on your credit accounts.
 - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
 - Receive and carefully review a free copy of your credit report by going to www.annualcreditreport.com.

Equifax
Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374
800-525-6285
securitymonitoring@equifax.com

Experian
Experian Security Assistance
P.O. Box 72
Allen, TX 75013
888-397-3742
businessrecordsvictimassistance@experian.com

TransUnion
Consumer Relations &
Fraud Victim Assistance
P.O. Box 2000
Chester, PA 19016
800-372-8391
databreach@Transunion.com

2. Carefully review all bills and credit card statements you receive to see if there are items you did not contract for or purchase. Also review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.
3. The Federal Trade Commission (“FTC”) offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft, such as by setting up fraud alerts or placing a “security freeze” on your credit accounts. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you should contact local law enforcement, and you can also contact the Fraud Department of the FTC, which will collect all information and make it available to law enforcement agencies. The FTC can be contacted at the website or phone number above, or at the mailing address below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue
NW Washington, DC 20580

4. *For Maryland Residents.* : You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.marylandattorneygeneral.gov.
5. *For North Carolina Residents:* You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.

6. *For Rhode Island Residents:* You may contact and obtain information from and/or report identity theft to your state attorney general at:

Rhode Island Attorney General's Office
150 South Main Street
Providence, RI 02903
Phone: (401) 274-4400
Website: www.riag.ri.gov

You have the right to obtain a copy of the applicable police report, if any, relating to this incident.