BakerHostetler

Baker&Hostetler LLP

Washington Square, Suite 1100
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5403

T 202.861.1500
F 202.861.1783
www.bakerlaw.com

Brian J. Craig
direct dial: 202.861.1662
bxcraig@bakerlaw.com

November 29, 2022

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

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

Re: Incident Notification

Dear Attorney General Frosh:

We are writing on behalf of our client, Alvarez Tax Services, LLC ("Alvarez"), to notify your office of a cybersecurity incident that involved Maryland residents' information.

On July 18, 2022, Alvarez became aware of a network security incident that temporarily impacted the availability of its computer systems. Upon identifying the activity, Alvarez initiated an incident response plan, took proactive steps to secure its network, and commenced an investigation with the assistance of a cybersecurity firm. The investigation revealed that an unauthorized party gained access to Alvarez's network and accessed and/or acquired files on some of its computer systems. Alvarez reviewed the files and, on October 4, 2022, determined the files contained the information of four Maryland residents, including their names and one or more of the following: Social Security numbers, bank account numbers, and routing numbers.

On November 29, 2022, Alvarez is providing notice via United States Postal Service First-Class mail to the Maryland residents in accordance with Md. Code Ann., Com. Law § 14-3504.[1] A copy of the notification is enclosed. Alvarez is offering complimentary one-year memberships to identity monitoring services through IDX to all Maryland residents whose Social Security numbers or driver's license numbers were involved in the incident. Alvarez has also established a dedicated call center for individuals to call with questions about the incident.

[1] This report does not waive Alvarez's objection that Maryland lacks personal jurisdiction over Alvarez related to this matter

To help prevent something like this from happening again, Alvarez has implemented additional safeguards and technical security measures to further protect and monitor their systems.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Brian J. Craig
Counsel

Enclosure

Alvarez Tax
Service LLC

P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-903-3648
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

November 29, 2022

<<NOTICE OF DATA BREACH>>

Dear <<FIRST NAME>> <<LAST NAME>>:

Alvarez Tax Service LLC is committed to protecting the confidentiality and security of the information we maintain. We are writing to notify you that we identified and addressed an incident that may have involved some of your personal information. We maintain your information because we provide accounting and tax preparation services. This notice explains the incident, measures we have taken, and additional steps you may consider taking in response.

What Happened? On July 18, 2022, we became aware of a network security incident that temporarily impacted the availability of our computer systems. Upon learning of this incident, we initiated our incident response plan, took proactive steps to secure our network, and commenced an investigation with the assistance of a cybersecurity firm. Our investigation revealed that an unauthorized party accessed and may have acquired certain files from our network as a result of this incident.

What Information Was Involved? We reviewed the files and, on October 4, 2022, determined, that one or more files contained your <<variable data>>.

What We Are Doing. As a precaution, we arranged for you to receive a complimentary <<one/two>>-year membership in credit monitoring services through IDX. This service includes tri-bureau credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. IDX is free and enrolling in this program will not affect your credit score.

To help prevent something like this from happening again, we have implemented additional safeguards and technical security measures to further protect and monitor our systems.

What You Can Do. We encourage you to remain vigilant by regularly reviewing your credit reports and financial account statements for any unauthorized activity. If you see activity you did not authorize, please contact the relevant financial institution immediately. You can also sign up for the complimentary credit monitoring services through IDX by calling 1-833-903-3648 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. Please note the deadline to enroll is **March 1, 2023**. For more information on identity theft prevention, please see the pages following this letter.

For More Information. For more information on identity theft prevention, please see the pages following this letter. If you have any questions, please call 1-833-903-3648, Monday through Friday, 6 a.m. to 6 p.m., Pacific Time.

Sincerely,

Antonio Alvarez
Co-Founding Partner

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com
Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Alvarez Tax Services, LLC can be contacted via mail at 640 N. Tustin Ave. Suite 104, Santa Ana, CA 92705, or by telephone at (714) 400-9201.

Additional information for residents of the following states:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.