



Melissa K. Ventrone
T (312) 360-2506
Email: mventrone@clarkhill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900

April 7, 2022

Via USPS

Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

We represent Miranda CPA, PLLC ("Miranda CPA") with respect to a data security incident involving the potential exposure of certain personally identifiable information described in more detail below. Miranda CPA is a full-service accounting and tax firm located in Richardson, Texas. Miranda CPA is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident in the future.

1. Nature of security incident.

On September 15, 2021, Miranda CPA learned of suspicious activity associated with one of its corporate email accounts. Miranda CPA immediately began an investigation to determine what occurred and whether any data was accessed or exfiltrated. The investigation was unable to determine whether any data was compromised. Miranda CPA then hired a vendor to conduct an in-depth review of the email account to identify any personal information that may have been located in the account. This review was completed on February 1, 2022. From this review, it appears the information in the email account may have included individuals' names and addresses in combination with one or more of the following data elements: Social Security numbers, date of birth, driver's license numbers, financial account information, passport numbers, IRS E-File PIN, and limited health information.

2. Number of residents affected.

Four (4) Maryland residents may have been affected and were notified of the incident. A notification letter was sent to the potentially affected individuals on April 7, 2022 (a copy of the form notification letter is enclosed as Exhibit A).

April 7, 2022

Page 2

3. Steps taken in response to the incident.

Miranda CPA took steps to address this incident and prevent similar incidents in the future. Miranda CPA changed the passwords to the affected corporate email account and multifactor authentication was enabled across all Miranda CPA corporate email accounts. Additionally, affected individuals were offered 12 months of credit monitoring and identity protection services through IDX.

4. Contact information.

Miranda CPA takes the security of the information in its control seriously and is committed to ensuring information within its control is protected. If you have any questions or need additional information, please do not hesitate to contact me at mventrone@clarkhill.com or (312) 360-2506.

Sincerely,

CLARK HILL



Melissa K. Ventrone
Member

cc: Mariah Leffingwell - mleffingwell@clarkhill.com

EXHIBIT A

MIRANDA CPA, PLLC
Return to IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223



Miranda CPA, PLLC

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: [XXXXXXXXXX]

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

April 7, 2022

Notice of Data Security Incident

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

Miranda CPA, PLLC ("Miranda CPA") recently experienced a data security incident that may have impacted some of your personal information described in more detail below. We may have your information if Miranda CPA prepared partnership returns or provided other tax services for an organization in which you hold an investment. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information and resources we are making available to help you.

What happened?

On September 15, 2021, we learned of suspicious activity associated with one of our corporate email accounts. As soon as we learned of this activity, we began an internal investigation to determine what occurred and whether any information may have been compromised. Unfortunately, the investigation was not able to determine whether any information was accessed or acquired as a result of this incident. Out of an abundance of caution, we hired a vendor to conduct an in-depth review of the email account to identify any personal information that may have been located in the account. This review was completed on February 1, 2022, at which point we determined that some of your personal information may have been present at the time of the incident. While we have no indication that any of your personal information has been misused, out of an abundance of caution, we wanted to inform you about this incident and provide you with resources to protect yourself.

What information was involved?

From the review, it appears that your name, <<Variable Text 1>> <<Variable Text >> may have been impacted by this incident.

What we are doing?

We want to assure you that we have taken steps to prevent this kind of event from happening in the future: Since the incident, the password to the affected corporate email account was changed and multifactor authentication was enabled across all Miranda CPA corporate email accounts. We also encourage all of our clients to use the secure file share system we have in place.

Although we do not believe there is any risk that your information will be misused, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <<12

EXHIBIT A

months/24 months>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id 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 remain vigilant for incidents of identity theft by reviewing your bank account and other financial statements as well as your credit reports for suspicious activity. You should also contact IDX with any questions and to take advantage of the IDX service offering. Please note the deadline to enroll in the services is May 7, 2022. Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

Again, at this time, there is no evidence that your information has been misused. 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:

Please call 1-800-939-4170 Monday through Friday from 8am – 8 pm Central Time for assistance or for any additional questions you may have. Your trust is our top priority and we deeply regret any inconvenience or concern this matter may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "William Miranda". The signature is stylized with a cursive script.

William Miranda
Miranda CPA, PLLC



Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> 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 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Single Bureau Credit Monitoring. You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call an IDX fraud specialist, who can help you determine if it's an indicator of identity theft.

5. Fraud Consultation. You have unlimited access to consultation with an IDX specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

6. Identity Theft Restoration. If you become a victim of identity theft, an experienced IDX licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

7. 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.

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.

8. 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
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-836-6351

www.equifax.com/personal/credit-report-services

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

TransUnion Fraud Reporting
P.O. Box 2000
Chester, PA 19022-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094
1-800-680-7289
www.transunion.com

EXHIBIT A

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.

9. 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.

10. 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.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

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/201904_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: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed in regard to this incident. There is one Rhode Island resident impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft