

Jason M. Schwent
T (312) 985-5939
F +13125177573
Email:jschwent@clarkhill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

June 2, 2023

Attorney General Brian E. Frosh
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Dear Attorney General Frosh:

We represent Desai & Shah, PC, CPA (“Desai & Shah”) as Outside Counsel with respect to a data security incident involving the potential exposure of certain personally identifiable information (“PII”) described in more detail below. Desai & Shah, a full service Certified Public Accounting firm located in Germantown, MD, is committed to answering any questions you may have about the data security incident, their response, and steps taken to prevent a similar incident from occurring in the future.

1. Nature of security incident.

In October 2022, Desai & Shah learned that some of the tax returns they filed on behalf of their clients were being rejected by the IRS as having already been filed. They immediately started an internal investigation to determine the possible cause of the issue and if any of their systems were compromised. They also hired an independent computer forensics firm to assist in their investigation. The investigation found unauthorized access to one employee’s computer but was unable to determine if any information in any Desai & Shah systems was accessed. While there was no evidence any information had been viewed, taken or otherwise accessed, out of an abundance of caution, Desai & Shah investigated what personal information may have been present in the potentially affected systems and if any individuals may have been impacted. This review was completed on April 24, 2023. From this review, it appears the information in the potentially affected systems may have included names, addresses, Social Security numbers, EIN/TIN numbers, and financial information generally found on tax returns or related documents.

2. Number of residents affected.

Five-hundred twenty-six (526) Maryland residents may have been affected and were notified of the incident. A notification letter was sent to the potentially affected individuals on June 2, 2023. A copy of the form notification letter is enclosed.

3. Steps taken in response to the incident.

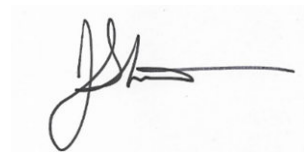
Since this incident, Desai & Shah replaced the affected computer, changed all employee passwords, implemented managed security services including endpoint detection and response and a managed security operations center, and strengthened multifactor authentication for remote access to Desai & Shah systems. Additionally, impacted individuals were offered 12 months of credit monitoring and identity protection services through Experian.

4. Contact Information

Desai & Shah takes the security of the information in its control seriously and is committed to ensuring it is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at jschwent@clarkhill.com or (312) 985-5939.

Sincerely,

CLARK HILL

A handwritten signature in black ink, appearing to read 'JS', followed by a long horizontal line extending to the right.

Jason M. Schwent



<<RETURN ADDRESS>>
<<City>>, <<State>> <<ZIP>>

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

<<Date>>

Notice of Data Security Incident

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

Desai & Shah, PC, CPA (“Desai & Shah”) is writing to let you know about a data security incident that may have affected your personal information. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this incident may cause you. This letter contains information about what occurred, steps you can take to protect your information, and resources we are making available to help you do so.

What happened?

In October 2022 we received information that some of the tax returns we filed on behalf of clients were being rejected by the IRS as having already been filed. We immediately started an internal investigation to determine the possible cause of the issue and if any of our systems were compromised. We also hired an independent computer forensics firm to assist in our investigation. The investigation found unauthorized access to one employee’s computer but was unable to determine if any information in our systems had been viewed, taken, or otherwise accessed. Out of an abundance of caution, we investigated what personal information may have been present in the potentially affected systems and if any individuals may have been impacted. This review was completed on April 24, 2023.

While we have no evidence that your personal information was actually compromised or misused, because it was present on the systems with unauthorized access, we wanted to notify you about this incident and provide you with resources to protect yourself.

What information was impacted?

From the review, it appears that your name, address, Social Security number, EIN/TIN numbers, and financial information generally found on your tax return or related documents 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 affected computer has been replaced, employee passwords have been changed, implemented managed security services including endpoint detection and response and a managed security operations center, and strengthened multifactor authentication across all Desai & Shah accounts.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for [##] months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for [##] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

How do I enroll for the free services?

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [##]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** [Enrollment End Date] (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [Enrollment URL]
- Provide your **activation code**: [Activation Code]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [Experian TFN] by [Enrollment End Date]. Be prepared to provide engagement number [B#####] as proof of eligibility for the Identity Restoration services by Experian.

What you can do:

It is always a good idea to remain vigilant and be on the look-out for evidence of identity theft or fraud, and to review your bank account and other financial statements as well as your credit reports for suspicious activity. We also encourage you to contact Transunion with any questions and to take full advantage of the Transunion service offering. 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.

As an additional layer of security, Desai & Shah strongly recommends you use multi-factor authentication for any online accounts containing financial or other sensitive information and obtain an Identity Protection PIN from the IRS by visiting the IRS website here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

For more information:

If you have any questions or concerns, please call [CALL CENTER #] Monday through Friday from 8 am – 8:00 pm Eastern Time. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Desai & Shah PC CPAs

Desai & Shah, PC, CPA

RECOMMENDED STEPS TO HELP PROTECT YOUR INFORMATION

ADDITIONAL DETAILS REGARDING YOUR [###]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

1. 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.

2. 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

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.

3. 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.

4. 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.

Florida Residents: Office of the Attorney General, State of Florida, PL-01 The Capitol, Tallahassee, FL 32399-1050; Telephone: 1-800-435-7352; <https://www.myfloridalegal.com>

Massachusetts Residents: Massachusetts Office of the Attorney General, Data Privacy and Security Division, One Ashburton Place, Boston, MA 02108; Telephone: 1-617-727-8400

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 Hampshire Residents: Office of the Attorney General, 33 Capitol St, Concord, NH 03301; Telephone: 1-603-271-3658

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.

Ohio Residents: The Office of the Attorney General, 30 E Broad St., 14th Floor, Columbus, OH 43215; Telephone: 1-800-282-0515; <https://www.ohioattorneygeneral.gov>

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 are 2 Rhode Island residents impacted by this incident.

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