CLARK HILL

Robert A. Stern
T 312.985.5940
F 312.985.5955
Email: rastern@clarkhill.com

Clark Hill
130 East Randolph Street
Suite 3900
Chicago, IL 60601
T 312.985.5900
F 312.985.5999

clarkhill.com

June 11, 2020

Office of the Attorney General
Consumer Protection and Anittrust
1050 E. Interstate Ave. Suite 200
Bismark, ND 58503-5574

Dear Attorney General Wayne Stenehjem:

We represent Gonzalez CPA with respect to a data security incident involving a limited number of fraudulent tax returns. Gonzalez CPA is committed to answering any questions you may have about the data security incident, its response, and steps it has taken to prevent a similar incident in the future.

1. Nature of security incident.

Beginning in March of 2020, Gonzalez CPA was informed that a limited number of firm clients could not file their tax returns as the IRS indicated that the returns had already been filed. Upon learning of these rejected returns, Gonzalez CPA hired an independent computer forensic investigator to determine if there was a compromise of its network or systems. To date, the forensic investigators have found no suspicious activity on Gonzalez CPA systems. Gonzalez CPA has also obtained logs from its tax software provider and requested they launch their own investigation. To date, there have been no indications of suspicious activity with its tax software provider either. While we continue to investigate what occurred, we wanted to promptly issue notice to all clients of Gonzalez CPA and offer resources to protect themselves.

2. Number of North Dakota residents affected.

One (1) North Dakota resident may have been affected and were notified of the incident. A notification letter was sent to the potentially affected individuals on June 11th, 2020 via regular mail (a copy of the form notification letter is enclosed).

3. Steps taken or plan to take relating to the incident.

Gonzalez CPA has contacted all individuals who had issues filing their returns and worked with them to fill out IRS Form 14039 at no cost to the Client. Gonzalez CPA has also offered twelve

201477

(12) months of credit monitoring and identity restoration services to all individual clients and their spouses. Since the incident, all passwords have been reset, a forensic investigation has occurred, an accounting of logins into Gonzalez CPA's tax software has been conducted, and Gonzalez CPA is working with its forensic investigator to determine other ways they can further enhance their cybersecurity protocols.

4. Contact information.

Gonzalez 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 Rastern@clarkhill.com or (312) 985-5940.

Very truly yours,

CLARK HILL

Robert Stern

Robert A. Stern

Enclosure

GONZALEZ CPA
EXPERTISE | KNOWLEDGE | TRUST

C/O ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

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

June 11, 2020

Notice of Data Breach

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

I wanted to let you know about a potential data security incident experienced by Gonzalez CPA that may have impacted your personal information. I value and respect the privacy of your information, 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 I am making available to help you.

What happened?

Beginning in March 2020, I learned that a limited number of my clients had experienced fraudulent tax filings. Upon learning of this fraud, I hired an independent computer forensic investigator to determine if there was a compromise of my network. To date, the forensic investigators have found no suspicious activity on my systems. We have asked our tax software provider to launch their own investigation as well. Our forensic investigation is ongoing, and I don't yet know whether any of your information was compromised, but I wanted to let you know before the investigation is complete so you can take steps to protect yourself.

What Information was involved?

Information that may be affected includes your tax return information, such as your name, address, Social Security number, bank account number if you provided that to me, and other tax related information.

What we are doing:

While the investigation is ongoing, I have arranged for you to receive credit monitoring and identity protection services at no cost to you provided by MyIDCare™ powered by ID Experts for 12 months.

What you can do:

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-800-939-4170 or going to https://app.myidcare.com/account-creation/protect and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 8 am - 8 pm Central Time. Please note the deadline to enroll is September 11, 2020.

How to Enroll: You can sign up online or via telephone.

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.

If you received a fraudulent deposit from the IRS into your bank account, the IRS has recommended the following:

1. Do not spend this money, as it must be returned to the IRS.
2. Contact your bank's fraud department and let them know that the money was deposited as a result of a fraudulent tax filing, and that the deposit should be reversed as soon as possible.
3. Do not return the money by check. The most reliable way for the money to be returned and credited to you is to instruct your bank to reverse the deposit.
4. If you have any issues with your bank and the return of the money, please contact me.

Additionally, if you know or suspect you are a victim of tax-related identity theft, the IRS recommends the following steps:

- Respond immediately to any IRS written notice. **The IRS will not contact you via phone.**
- If you received a Letter 4883C from the IRS indicating that they received a suspicious tax return with your name on it, you should follow the instructions on that letter to verify your identity with the IRS. Once you verify your identity, you can advise the IRS that you did not file the suspicious tax return. Additionally, you may be asked to file a paper return for the current filing season.
- If you believe you may be a victim of tax fraud but have not received a Letter 4883C from the IRS, you should fill out and submit IRS Form 14039, which is available at IRS.gov. I can provide you with a copy of that form and assist you with filling it out if you would like. If you plan on filing on extension, please contact me for more information.

If you previously contacted the IRS and did not have a resolution, contact the IRS for specialized assistance at 1-800-908-4490. The IRS has teams available to assist. You should also visit https://www.irs.gov/individuals/how-irs-id-theft-victim-assistance-works for more information.

The security of your information is of the utmost importance to me. Once the forensic investigation is completed, I will be working closely with the investigators to identify additional security measures to further enhance the security of my system.

Other important information:

If you have any questions or concerns, please call 1-800-939-4170 Monday through Friday, 8 am - 8 pm Central Time. Your trust is a top priority for me, and I deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

John Gonzalez, CPA

MyIDCare™

Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Go to https://app.myidcare.com/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 MyIDCare 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, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare 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. 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 MyIDCare, notify them immediately by calling or by logging into the MyIDCare 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.

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	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.alerts.equifax.com	www.experian.com	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 (http://www.ca.gov/Privacy) for additional information on protection against identity theft.

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.

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

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