Clark Hill

Melissa K. Ventrone
T (312) 360-2506
F (312) 517-7572
Email:mventrone@ClarkHill.com

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

July 6, 2021

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Dear Attorney General Formella:

We represent Cronin, Hanley & VanZile, LLC ("CHV") with respect to a potential data security incident involving a limited number of fraudulent tax returns. CHV 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.

In late April 2021, CHV learned that tax returns for a limited number of clients could not be filed as the IRS indicated that the returns had already been filed. Upon learning of these rejected returns, CHV hired an independent computer forensic investigator to determine if there was a compromise of their network or systems. Taxpayers with fraudulent returns filed were immediately notified of the fraudulent filing and investigation.

To date, the forensic investigators have not found any suspicious activity on CHV's systems, although the investigation did determine that a limited number of fraudulent returns were filed using CHV's tax software. Regardless, CHV wanted to notify all clients and dependents of the investigation and provide them with resources to help them protect themselves. Information that may have been impacted includes names, addresses, Social Security numbers, bank account numbers and other tax related information.

2. Number of residents affected.

One (1) New Hampshire resident may have been affected and was notified of the incident. A notification letter was sent to the potentially affected individual on July 6, 2021 via regular mail (a copy of the form notification letter is enclosed).

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

CHV has notified all impacted individuals and offered twelve (12) months of credit monitoring and identity restoration services. All passwords have been reset, a forensic investigation is in process, and CHV is working with its forensic investigator to determine other ways they can further enhance their cybersecurity protocols. Finally, CHV is working with the IRS to produce a list of all clients and their dependents so that the IRS can add additional precautions to those individuals' returns.

4. Contact information.

CHV 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.

Very truly yours,

CLARK HILL

Melissa K. Ventrone
cc: Robert A. Stern

Enclosure

Cronin, Hanley & VanZile, LLC
Return to IDX
10300 SW Greenburg Rd., Suite 570
Portland, OR 97223

To Enroll, Please Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

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

July 6, 2021

Notice of Data Breach

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

We wanted to let you know about a data security incident experienced by Cronin, Hanley & VanZile, LLC ("CHV") that we are in the process of investigating. 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?

We recently became aware that tax returns for a limited number of clients were fraudulently filed under our Electronic Filing Identification Number (EFIN). We immediately began an investigation to determine if this was related to our systems, and hired independent computer forensic experts to assist us with our investigation. We don't know whether there was a compromise of our tax systems and do not believe your data was impacted but wanted to let you know about this incident out of an abundance of caution.

What information was involved?

We store information necessary to file your taxes in our tax system. This includes your name, address, Social Security number, and bank account information if you provided it to us for use to pay a tax liability or receive a refund.

What are we doing?

The security of our systems and your information is important to us, and we wanted you to know that prior to this incident we had invested significant resources in our network. Over the past couple years, we invested in new servers and technology to provide for additional security. We work with an external IT company that provides 24/7 monitoring of our servers and computers, use a secure mail service provider for correspondence, and use a secure portal that is directly connected with our tax software provider Intuit Lacerte. We have antivirus installed on all servers and computers, and train employees on recognizing and responding to cybersecurity threats.

Out of an abundance of caution, we have conducted a system wide password reset, implemented multi-factor authentication on all accounts, and obtained a new EFIN. We are currently working with the IRS to further protect our clients by opting into the Practitioner Relief Program, which enables CHV to notify the IRS in advance of a filing for verification purposes. Additionally, we will be working closely with the forensic investigators to identify security controls

to help tighten the security of our systems. We can assure you that if there is an issue with the security of our systems, we are committed to taking steps to prevent this type of thing from occurring again.

We have also arranged for you to receive identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 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 can you do?

It is always a good idea to review your bank account and other financial statements, and immediately contact your financial institution if you identify suspicious activity. We encourage you to enroll in free IDX identity protection services by going to https://app.idx.us/account-creation/protect or calling 1-800-939-4170 and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is October 6, 2021.

For More Information.

Please let us know if you receive a letter from the IRS. **The IRS will not contact you via phone.** If you have any questions or concerns, please call 1-800-939-4170 Monday through Friday from 9 am - 9 pm Eastern Time. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Maryann Hanley & Cara VanZile
Cronin, Hanley & VanZile, LLC

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. 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 IDX identity protection, notify them immediately by calling or by logging into the IDX 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.

4. 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.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.

5. 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.

6. 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.

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.

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.