BROOKS PIERCE
FOUNDED 1897

WELLS FARGO CAPITOL CENTER
150 FAYETTEVILLE STREET, SUITE 1700
RALEIGH, NC 27601

T 919.839.0300
F 919.839.0304
WWW.BROOKSPIERCE.COM

March 28, 2022

Sent Via FedEx

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: *Notice of Data Security Breach – Gerald O. Dry, P.A.*

To Whom It May Concern:

I am writing on behalf of our client, Gerald O. Dry, P.A., a North Carolina accounting firm located at 211 Le Phillip Ct NE, Concord, NC 28025 (the "Firm"). I write to notify you, pursuant to N.H. Rev. Stat. Ann. § 359-C:19 *et seq.*, of a data security incident involving five (5) New Hampshire residents.

Discovery and Nature of Breach

On February 3, 2022, the Firm began to experience an abnormally high rejection rate when electronically filing clients' federal tax returns. On Monday, February 7, 2022, a few days after the Firm first began to notice this increased rejection rate, Intuit, Inc., the Firm's tax preparation software provider, contacted the Firm to inform it of potentially suspicious activity. Intuit represented that federal tax returns for ten (10) filers that had been prepared and filed by the Firm in prior tax seasons had been submitted for electronic filing on February 3, 2022, through the Intuit account of another accounting firm that was believed to have experienced a data breach.

Given the concurrence of the increased filing rejection rate and Inuit's notice, the Firm quickly sought assistance from industry professionals, including from counsel submitting this notice and from a qualified cyber forensics investigator. On February 18, 2022, after a thorough analysis of the available forensic logs, it was discovered that the Firm's server, where all tax returns are stored prior to filing, was compromised in 2021 by the introduction of malware that could have allowed an unauthorized person to gain remote access. This malware was automatically removed by endpoint protection software installed by the Firm's third-party managed IT provider on or about June 8, 2021.

The unauthorized person may have gained access to any information used to file a tax return including, name, Social Security Number, driver's license number, date of birth, address, and employment (W-2 and 1099) information, as well as direct deposit bank account information,

including account number and routing information (if that information was provided). Additionally, the information of any other persons, such as spouses or dependents, appearing on a filer's return may have been exposed.

The Firm's Response

Immediately after hearing from Intuit on February 7, the Firm implemented various security measures to further secure their network and systems. These measures included, but were not limited to:

- Requiring all users to change their network passwords;
- Implementing two-factor authentication for all users before they could access the Intuit ProSeries software and/or their Microsoft 365 accounts; and
- Implementing two-factor authentication for its Sonic Wall Global VPN.

This is an ongoing process and, moving forward, the Firm will work with trusted third-party IT providers to implement additional technical security measures and will redouble its efforts to train employees in cybersecurity best practices.

In addition to taking steps to further strengthen its IT infrastructure, the Firm has also taken steps to protect its customers' data and work with them to address any issues with the IRS or state tax departments. These steps include:

- Communicating with the IRS and the Federation of Tax Administrators regarding this incident and cooperating to process client returns in the most expeditious, efficient, and secure way possible;
- Working with affected clients to ensure their returns are filed in a timely manner;
- Contacting the FBI Field Office in Charlotte, North Carolina, to apprise them of this incident; and
- Continuing to work to identify if any other clients were affected.

Notice to Affected Clients and Credit Monitoring

The Firm mailed formal notice of this incident to individual tax filer clients and their spouses in substantially the same form as the enclosed letter. This notice was mailed on March 25, 2022.

The Firm is offering all potentially affected individuals a complimentary one-year membership in credit monitoring and identity theft protection services from IDX. This offering

includes one year of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services.

Contact Information

If you have any other questions or need additional information, please let me know.

Sincerely yours,

S. Wilson Quick

Enclosure
1 – Sample Consumer Notification Letter

Gerald O. Dry, PA
Certified Public Accountants
P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-599-2436
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<Enrollment>>

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

March 25, 2022

Notice of Data Breach

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

Gerald O. Dry, PA (the "Firm") recently discovered an incident that may have affected the security of your personal information. We take this incident seriously, and write to provide you with information about the incident, steps we are taking in response, and steps you can take to better protect against the possibility of identity theft and tax fraud.

What Happened

On February 7, 2022, the Firm was notified by our professional tax preparation software provider, Intuit Inc., of suspicious filing activity relating to ten tax returns for individuals for whom the Firm has prepared tax returns in the prior tax season. Following this notice, the Firm launched an investigation with guidance from third-party cybersecurity experts to determine the nature and scope of the incident. On February 18, 2022, it was discovered that malware introduced onto our server last year and removed by June 8, 2021, may have permitted access to databases where we store information necessary to prepare and file tax returns.

What Information Was Involved

Our tax preparation software contained the information necessary for us to prepare and respond to inquiries regarding prior year tax returns. This information may have included your name, Social Security Number, driver's license number, date of birth, familial information (including information about spouses or dependents), address, and employment information, as well as direct deposit bank account information, including account number and routing information if any of that information was provided to us. Because your information was stored in our systems we are sending you this notice out of an abundance of caution to help you take appropriate steps to protect your identity.

What We Are Doing

We take this incident and the security of the personal information we maintain seriously. Following notice from Intuit, the Firm immediately took steps to secure access to our tax preparation software and all other systems that may contain personal information by resetting passwords and turning on two-factor authentication for all users, where available. We also brought in third-party professionals to investigate. With the help of a computer forensics specialist, we confirmed that there is no malicious software present on or suspicious activity in our systems at the current time.

We have already notified the Internal Revenue Service and the Federal Bureau of Investigation about this incident and are in the process of notifying relevant state agencies. We will cooperate with any government investigation that is opened moving forward. We have also provided information about this incident and our past tax return filings to the IRS so that they may monitor filings for and provide assistance to our clients and their families.

In addition, we are offering complimentary identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <<12 or 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

You are encouraged to remain vigilant against identity theft by regularly reviewing financial account statements and monitoring credit reports for suspicious activity. Additionally, be vigilant in communicating with others about your tax information. The IRS will not make contact by Email or text message and will only call in very rare circumstances, usually after they have sent a letter indicating that a telephone call will follow. If you receive funds from the IRS that you were not expecting, either because you have not yet filed a tax return or the amount is different from what you were expecting, you should not spend that money until you have notified the IRS. The Firm is available to assist you with resolving this and other issues with filing tax returns.

We also encourage you to contact IDX with any questions and to enroll in the complimentary identity protection services being offered by calling 1-833-599-2436 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. Please note the deadline to enroll is June 25, 2022.

Please also review the enclosed "Recommended Steps to help Protect your Information" for detailed instructions on how to enroll and to learn about additional steps to take to help protect personal information. 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.

For More Information

We understand there may be questions that are not answered by this letter or the enclosed information. You may contact an IDX representative by calling 1-833-599-2436 Monday through Friday from 9 AM to 9 PM Eastern Time to speak with someone familiar with this incident and the identity protection enrollment process.

Of course, you may also wish to speak with one of our accountants about the impact of this incident on filing taxes. Please feel free to contact us as you normally would with those questions.

We sincerely regret that this incident occurred, and we apologize for any inconvenience it may have caused you.

Respectfully,

Gerald O. Dry Jr.

Gerald O. Dry, Jr., CPA

(Enclosure)

Recommended Steps to help Protect your Information

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.

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.

Telephone. Contact IDX at 1-833-599-2436 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Watch for Suspicious Activity. 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 the IDX 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 your state attorney general.

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 online or by phone. 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:

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.

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.

Notify law enforcement of any suspicious activity. You should also notify the appropriate law enforcement authorities, your state attorney general, and/or the U.S. Federal Trade Commission (FTC) of any suspected identity theft.

Obtain an IP Pin from the IRS. If you have not already been contacted by the IRS regarding additional steps to protect your identity, you may wish to obtain an IRS identity protection PIN to aid in the prevention of fraudulent tax returns being filed using your information. You may visit https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin to learn more about this option.

Additional resources to protect against identity theft. You can find additional information to help protect against identity theft by contacting the 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. Depending upon your state residency you may also be able to obtain additional information from the agencies below.

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 Residents: Office of the Attorney General for the District of Columbia, 400 6th Street, NW, Washington, DC 20001, https://oag.dc.gov/, Telephone: 1-202-727-3400.

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 York Residents: 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; 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, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-877-566-7226.

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