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

July 13, 2022

Sent Via FedEx

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

Re: *Update to 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. (the "Firm"), a North Carolina accounting firm located at 211 Le Phillip Ct NE, Concord, NC 28025. Pursuant to N.H. Rev. Stat. Ann. § 359-C:19 *et seq.*, I am writing to update you about a data security incident involving two (2) New Hampshire residents. The Firm originally provided notice to your office on March 28, 2022, that five (5) residents were affected.

This data security incident stems from a malicious malware attack on the Firm's servers where taxpayer information was kept. In February 2022, the Firm began to experience an abnormally high rejection rate when electronically filing clients' federal tax returns. The Firm then received notice from Intuit, the Firm's tax handling software vendor, of possible suspicious activity. The Firm quickly began an investigation and, 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 removed by endpoint protection software installed by the Firm's third-party managed IT provider on or about June 8, 2021.

The Firm first mailed formal notice of this incident to individual tax filer clients and their spouses. This notice was mailed on March 25, 2022.

Thereafter, the Firm conducted a careful review of its remaining records to identify any additional individuals whose information may have been compromised. Following this review, it was determined that two (2) additional New Hampshire residents were affected. These individuals were dependents of primary tax filers notified in the Firm's initial round of notifications. Notice, in substantially the same form as the enclosed sample letter, was mailed to these individuals' parent/guardian on July 6, 2022.

Email: wquick@brookspierce.com Direct Dial: 919-573-6213 Fax: 336-232-9214
Brooks, Pierce, McLendon, Humphrey & Leonard, L.L.P.
Attorneys and Counsellors at Law

The Firm is offering all potentially affected persons a complimentary one-year membership in identity theft protection services from IDX. This offering includes CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. Additionally, all adults who register with IDX will receive credit monitoring for the duration of the identity theft protection services.

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 for Minors

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>>

To the Parent or Guardian of
<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

July 6, 2022

Notice of Data Breach

Dear Parent or Guardian of <<FIRST NAME>> <<LAST NAME>>,

Gerald O. Dry, PA (the "Firm") recently discovered an incident that may have affected the security of the above-named minor's 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. Following a careful review of potentially exposed information, we discovered that the above-named minor's information was accessible because we file taxes for someone who claimed that minor as a dependent on their tax return.

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 the above-named minor's name, date of birth, and Social Security Number. Because your minor's 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 their 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, the Federal Bureau of Investigation, and relevant state agencies

about this incident. 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 and the state Federation of Tax Administrators 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 months/24 months>> of CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help resolve issues if the above-named minor's identity is compromised.

What You Can Do

You are encouraged to remain vigilant against identity theft by regularly reviewing financial account statements for suspicious activity. Additionally, be vigilant in communicating with others about 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 the above-named minor receives funds from the IRS that are not expected, either because they have not yet filed a tax return or the amount is different from what they were expecting, they should not spend that money until the IRS has been notified. The Firm is available to assist you or the minor directly with resolving this and other issues with filing tax returns.

We also encourage you to contact IDX with any questions and to help the above-named minor 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 October 6, 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 or your family.

Respectfully,

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.

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 identity.

Watch for Suspicious Activity. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports (if you have an established credit profile).

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.

Security Freeze. Typically, minors do not have an established credit file. You may, however, place a free credit freeze for minors with the national credit reporting bureaus. By placing a security freeze, someone who fraudulently acquires a minor's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact the three national credit reporting bureaus listed below 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 child's credit files. 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

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