MAINE SECURITY BREACH REPORTING FORM
PURSUANT TO ME. STAT. § 1348

ATTACHMENT 2

GERALD O. DRY, P.A.

***

This attachment provides additional details relating to a data security incident in which it is believed that an unauthorized third party gained access to an electronic database used by Gerald O. Dry, P.A. (the "Firm"). The Firm provides its clients with accounting and tax preparation services from its location in Concord, North Carolina.

Discovery and Nature of Breach

Beginning on the afternoon of Thursday, February 3, 2022, and continuing through Monday February 7, 2022, the Firm encountered an error message that prevented it from electronically filing federal tax returns.

After 5 PM EST on Monday, February 7, 2022, 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 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 an accounting firm in California that was believed to have experienced a data breach. Since initially learning of this suspicious activity, the Firm has encountered a higher than normal rate of rejected returns when trying to electronically file on behalf of clients and/or been provided with copies of IRS letters sent to clients who had not yet filed taxes for 2021. The Firm has worked directly with each of these clients to individually address their questions, report fraudulently filed returns, and ensure that the correct returns are filed and processed with all required information. This typically involves at least one telephone call with an affected client.

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. A review of the applicable database revealed that the personal information of five (5) Maine residents was accessible.

The Firm's Response

Immediately after hearing from Intuit on February 7th, the Firm implemented various security measures to further secure their network and systems. These measures included requiring all users to change their network passwords and implementing two-factor authentication for all users before they could access the Intuit ProSeries software and/or their Microsoft 365 accounts. The Firm has also decided to implement two-factor authentication for its Sonic Wall Global VPN. This is an ongoing process. 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.

The Firm has communicated with the IRS regarding this incident and is cooperating with them to process client returns in the most expeditious, efficient, and secure way possible. The Firm also contacted the FBI Field Office in Charlotte, North Carolina, to apprise them of this incident. They have asked to be periodically updated. The Firm will continue to cooperate with the IRS, state tax departments and consumer protection offices, and law enforcement regarding this incident through the current tax season and beyond.

Notice to Clients

On March 25, 2022, the Firm will mail formal notice of this incident to individual tax filer clients and their spouses in substantially the same form as the enclosed letter. The Firm continues to review its files to determine if additional persons should be notified.

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.

If you have any other questions or need additional information, please contact:

Will Quick, Esq.
Brooks, Pierce, McLendon,
Humphrey & Leonard, LLP
150 Fayetteville Street
1700 Wells Fargo Capitol Center
Raleigh, NC 27601
(919) 839-0300
E-mail: wquick@brookspierce.com