

February 25, 2019

Gregory J. Bautista
914.872.7839 (direct)
Gregory.Bautista@wilsonelser.com

Sent Via Regular Mail

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03302

Re: Data Security Incident

Dear Attorney General MacDonald:

We represent DiPardo Eremic & Co. CPA's ("DiPardo Eremic") with respect to an incident involving the potential exposure of certain personal information described in detail below.

1. Nature of the possible security breach or unauthorized use or access

On October 10, 2018, DiPardo Eremic discovered that some clients had tax returns filed by an unknown, unauthorized third party. Upon learning of this, DiPardo Eremic immediately contacted their tax preparation software provider and engaged computer experts to investigate whether their systems were at risk. Although a full examination of their systems has not identified evidence of compromise to clients' information, it is possible that personal information, including names, Social Security numbers and tax information may have viewed or accessed by an unknown and unauthorized third party. Accordingly, DiPardo Eremic is providing this notification as a courtesy to the Office of the New Hampshire Attorney General.

2. Number of New Hampshire residents potentially affected

Approximately two (2) New Hampshire residents were affected in this potential incident. DiPardo Eremic sent the potentially impacted individuals letters notifying them of this incident on February 25, 2019. A copy of the notification sent to the potentially impacted individuals is included with this letter, which informs these New Hampshire residents about the 12 months of credit monitoring and identity theft protection services that is being offered to them.

3. Steps DiPardo Eremic has taken or plans to take relating to the potential incident

Upon learning of this issue, DiPardo Eremic immediately engaged computer experts to investigate if its systems were at risk, and has been cooperating with the IRS in its investigations. DiPardo Eremic has also

1133 Westchester Avenue • White Plains, NY 10604 • p 914.323.7000 • f 914.323.7001

Albany • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston • Kentucky • Las Vegas • London
Los Angeles • Miami • Michigan • Milwaukee • New Jersey • New Orleans • New York • Orlando • Philadelphia • San Diego • San Francisco • Stamford • Virginia
Washington, DC • West Palm Beach • White Plains

wilsonelser.com

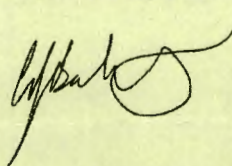
taken steps to continue to secure clients' information and their software provider has implemented enhanced encryption protection for all of their clients.

4. Other notification and contact information.

If you have any additional questions, please contact me at Gregory.Bautista@wilsonelser.com or (914) 872-7839.

Very Truly Yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Gregory J. Bautista



**DIPARDO EREMIC
& COMPANY, P.C.**
CERTIFIED PUBLIC ACCOUNTANTS

Daniele R. DiPardo, C.P.A.
Keith R. Eremic, C.P.A.
Michael A. Masters, C.P.A.

2901 Banksville Road, Pittsburgh, PA 15216 • Phone 412.341.7300 • Fax 412.341.2247

February 25, 2019

First name][last name]
[Street_Address]
[City][State][Zip]

Dear [First Name][Last name]:

We are writing to inform you of an incident involving unauthorized access to your personal information, including your name, address, Social Security number and related tax information. We take the security of your information very seriously and sincerely regret any inconvenience this may cause you. This letter contains information about what occurred, steps you can take to protect your information and resources we are making available to help you do that.

On October 10, 2018, we discovered that a small handful of our clients had tax returns filed by an unknown, unauthorized third party. We immediately contacted our tax preparation software provider and engaged forensic cyber experts to investigate the source of this activity, the magnitude of the fraudulently filed returns and whether our systems were at risk. In addition, we promptly submitted on your behalf a Form 14039, Identity Theft Affidavit, which informs the IRS of the fraudulent activity. As you are aware, we requested that you sign another copy of this form and we submitted it again to the IRS, along with those who had not filed their 2017 returns.

Because we value you and the safety of your information, out of an abundance of caution, we have arranged with **CyberScout**, an identity theft education and resolution specialist, to provide you with **Single Bureau Credit Monitoring** and **Triple Bureau Credit Report**¹ services at no cost to you. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your Experian credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. To enroll in these free services, please log on to <https://www.myidmanager.com> and follow the instructions provided. When prompted, please provide the following unique code to receive services: <CODE HERE>

We assure you that we have taken steps to secure our systems with the latest security protocols and are pleased to report that our swift action has stopped the issuance of unauthorized refunds. This includes changing our IRS EFIN numbers and resetting employees' access credentials for our computers and tax preparation software. In addition, our software supplier has implemented enhanced encryption protection for all of their clients to ensure that best practices to safeguard personal information are being followed.

We sincerely regret any inconvenience that this incident may cause you, and remain dedicated to protecting your personal information. Should you have any questions or concerns, or to obtain additional information about the free services described above, please call the CyberScout help line at 1-800-405-6108 and provide the fraud specialist with your unique code.

If you desire to contact us directly to aid you in this matter, or if you have any questions that we have not answered previously, please don't hesitate to reach out to us. We are here to service you in all matters, and especially in protecting your information.

Sincerely,
DiPardo Eremic & Co. CPA's
Daniele R. DiPardo CPA

¹ These services require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia*:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Maryland, Rhode Island, Illinois, and North Carolina*:

You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

Rhode Island Office of the Attorney General
Consumer Protection
150 South Main Street
Providence RI 02903
1-401-274-4400
www.riag.ri.gov

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Ave, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf) or Experian (<https://www.experian.com/fraud/center.html>). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.freeze.equifax.com
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.