WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

October 30, 2020

Robert F. Walker
601.499.8083 (direct)
Robert.Walker@wilsonelser.com

Via E-Mail

NH Department of Justice
Gordon J. MacDonald, Attorney General
33 Capitol Street
Concord, New Hampshire 03301
attorneygeneral@doj.nh.gov

Re: Potential Security Incident Involving L.A. Tax Service, LLP

Dear Attorney General MacDonald:

We represent L.A. Tax Service, LLP ("LATS"), an office providing tax services in Los Angeles, California. This letters constitutes LATS' notice following a potential business email compromise incident, which led to the fraudulent filing of approximately 50 tax returns on behalf of LATS' clients. Despite the fact that only 50 tax returns were fraudulently filed, LATS will notify all its 2018 and 2019 clients after a forensic investigation reveal potential access of LATS' data. Notice to the impacted individuals will be mailed by November 13, 2020.

1. **Nature of the incident.**

On September 15, 2020, LATS was notified by Lacerte Intuit, which is LATS' tax software, that some tax returns pertaining to LATS clients were fraudulently filed. To date, LATS is aware of approximately 50 tax returns fraudulently filed. LATS immediately contacted the 50 individuals whose tax returns were fraudulently filed. Upon receipt of Lacerte Intuit's notification, LATS promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. The forensic investigation was completed on October 7, 2020, revealing that tax returns of their clients were potentially exposed to an unauthorized third party in June 2020 and September 2020 following the receipt of a potential phishing email. After an internal investigation concluded on October 16, 2020, we determined that approximately 2604 individuals may have been impacted by the incident. Based on the investigation, it appears the exposed information may include the information present on LATS clients' tax returns (including names, addresses, taxpayer information and social security numbers). Out of an abundance of caution, LATS will notify all individuals by November 13, 2020.

2. **Number of New Hampshire residents affected.**

Two (2) New Hampshire residents were potentially affected by the incident. An incident notification letter addressed to the New Hampshire residents will be mailed by November 13, 2020. A sample copy of the Incident notification letter being mailed to potentially affected residents of New Hampshire is included with this letter at **Exhibit A**.

3. **Steps Taken In Response to the Incident.**

LATS takes the privacy and security of their information very seriously, and has taken steps to protect the privacy and security of potentially impacted individuals' information. Upon discovery of the incident, LATS immediately informed our law firm, Wilson Elser Moskowitz Edelman & Dicker LLP, and began identifying the individuals potentially impacted by the incident. Furthermore, LATS changed passwords to its email accounts, computers and servers; added multi-factor authentication to its email accounts; installed the Webroot anti-virus on all workstations for centralized management (removing users from being local admin of computers, creating an AD user that has local admin to avoid login to computers and cache credentials during software installations). Additionally, LATS is in the process of upgrading its email license to include spam filtering, updated firewall and anti-virus. Moreover, as outlined in the sample notification attached hereto, LATS provided the impacted individuals with complimentary services to help protect their identity. Specifically, LATS has arranged for the impacted individuals to enroll in credit and identity theft monitoring services at no cost to them for two years.

4. **Contact information.**

LATS remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Robert.Walker@WilsonElser.com or 601-499-8083.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Robert F. Walker

Robert F. Walker

Enclosures

EXHIBIT A

L. A. TAX SERVICE, LLP

C/O IDX
<<Address 1>>
<<City>><<State>><<Zip>>
<<Country>>

To Enroll, Please Call:
1-833-791-1659
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code:<<XXXXXXXX>>

<<First Name>><<Last Name>>
<<Address 1>><<Address 2>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Security Incident

Dear <<Name 1>>:

This letter is to notify you that L.A. Tax Service, LLP ("LA Tax Service") was the victim of a data security incident that might have resulted in unauthorized access to some of your personal information. We take the privacy and protection of your personal information very seriously. We regret any inconvenience this may cause. This letter contains information about what happened, steps we have taken, and resources we are making available to you to help protect your identity.

What happened and what information was involved:

On September 15, 2020, we were notified by Lacerte Intuit, our tax software, that some tax returns pertaining to our clients were fraudulently filed. To date, we are aware of approximately 50 tax returns fraudulently filed. If your tax return was among these 50 tax returns, we already notified you.

Upon receipt of Lacerte Intuit's notification, LA Tax Services promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. The forensic investigation was completed on October 7, 2020, revealing that tax returns of our clients were potentially exposed to an unauthorized third party in June 2020 and September 2020. After an internal investigation concluded on October 16, 2020, we determined that you were among the individuals potentially impacted by the incidents.

Based on the investigation, it appears the exposed information may include the information present on your tax return, such as your name, address, taxpayer information and social security number. Out of an abundance of caution, we wanted to inform you of this incident.

What we are doing and what you can do:

We take the privacy and security of your information very seriously. Upon discovery of this incident, we immediately changed all computer passwords and improved our computer security settings by enabling of a two-factor authentication for our emails. We also installed the Webroot anti-virus on all our workstations for centralized management (removing users from being local admin of computers, creating an AD user that has local admin to avoid login to computers and cache credentials during software installations). Additionally, we are upgrading our email license to include spam filtering, updated firewall and anti-virus.

We are also offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 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.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-791-1659 or going to https://app.idx.us/account-creation/protect 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 [Enrollment Deadline].

If you are a minor or if you claimed any minor dependents on your tax return, we are offering identity theft protection services to you/minor dependents through IDX including: 24 months of fully managed id theft recovery services and a $1,000,000 insurance reimbursement policy. Each minor received a separate letter with an individual code to activate the above-listed services.

You can also obtain an Identity Protection PIN (IP PIN) with the IRS by following the instructions at this link: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin .

For more information:

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 about this incident, please contact 1-833-791-1659 between 9:00 a.m. and 9:00 p.m. Eastern Standard Time for more information.

Sincerely,

_____

Esther Eisenstein, CPA
Aaron Rubenstein, EA
For L.A. Tax Service, LLP

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, New York, 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
New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

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); TransUnion (https://www.transunion.com/fraud-alerts); 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
https://www.equifax.com/personal/credit-report-services/credit-freeze/
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.