

September 16, 2021

Via Certified Mail; Return Receipt Requested

Attorney General John Formella
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Data Security Incident

Dear Attorney General Formella:

We represent Ives Sultan & Spike CPAs (“ISS”) with respect to a potential data security incident described in more detail below. ISS, provides accounting, auditing, tax planning, and business advisory services and is located in Woodbury, New York. ISS takes the security and privacy of their customers’ information very seriously and has taken steps to prevent a similar incident from occurring in the future.

1. Nature of the security incident.

Sometime in October 2020, ISS became aware of a potential business email compromise in connection with an unauthorized access since May 2020. We immediately engaged a third-party professional cybersecurity forensics team to conduct a thorough investigation into our entire email tenant. Through this investigation, ISS confirmed that an unknown party did gain unauthorized access to an ISS employee’s email account.

The forensic investigation concluded on October 20, 2020. On January 12, 2021, ISS’s carrier approved a vendor to conduct the automated term search. On January 26, 2021, ISS engaged an automated term search vendor to identify the type of PII in the compromised mailbox. On February 16, 2021, the automated term search concluded. On March 24, 2021, ISS’s carrier approved a manual review vendor to identify the affected individuals and the associated PII that was in the compromised mailbox. On March 31, 2021, the manual review vendor was engaged. On June 10, 2021, ISS’s carrier approved the manual review vendor to conduct an address research to locate missing addresses. On July 6, 2021, the manual review concluded. On July 28, 2021, ISS’s carrier approved a vendor to mail notice, establish a call center, and provide credit monitoring. On July 30, 2021, the vendor was engaged. On August 24, 2021, the notification list was finalized. On September 16, 2021, notice was mailed to the affected individuals. Based on the investigation, it appears that personal information was contained in the compromised mailbox consisting of Social Security Number, Driver’s License Number, and Financial Account information.

2. Number of New Hampshire residents affected.

A total of eleven (11) New Hampshire residents may have been potentially affected by this incident. Notification letters to these individuals were mailed on September 16, 2021 by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps taken.

ISS takes the security and privacy of the information very seriously, and has taken steps to prevent a similar event from occurring in the future, as well as to protect the privacy and security of potentially impacted individuals' information, including but not limited to: continuing to enhance security measures and providing cyber security training to its staff; and implementing Multi-Factor Authentication. ISS is also providing the potentially impacted individual with identity theft protection and credit monitoring services for a period of twelve (12) months at no cost.

4. Contact information.

ISS 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 Anjali.Das@wilsonelser.com or (312) 821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Anjali C. Das

Enclosure



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

Notice of Data Security Incident

We are writing to inform you of a data security incident involving Ives Sultan & Spike CPAs (“ISS”) that may have resulted in the unauthorized access to some of your personal information. ISS takes the security of your personal information very seriously, and we sincerely apologize for any inconvenience this incident may cause. This letter contains information about the incident and steps you can take to protect your information.

What Happened:

Sometime in October 2020, ISS became aware of a potential business email compromise in connection with an unauthorized access since May 2020. We immediately engaged a third-party professional cybersecurity forensics team to conduct a thorough investigation into our entire email tenant. Through this investigation, ISS confirmed that an unknown party did gain unauthorized access to an ISS employee’s email account.

What Information Was Involved:

Based on the investigation, it appears that some of your personal information was contained in the employee’s compromised email account, including your name, Social Security number, driver’s license and/or state identification number, and/or financial account information. While we do not have any evidence of the misuse of your information, we are nonetheless notifying you out of an abundance of caution and encourage you to take full advantage of the services offered.

What We Are Doing and What You Can Do:

ISS takes the protection and proper use of your information very seriously. Ensuring the safety of your data is of the utmost importance to us, and we sincerely regret any inconvenience or concern that this may cause. We take the security of all information in our control very seriously and are taking steps to prevent a similar event from occurring in the future, including but not limited to: continuing to enhance security measures and providing cybersecurity training for our staff; and implementing Multi Factor Authentication. In light of this incident, we have secured the services of TransUnion® to provide Single Bureau Credit Monitoring Services at no cost to you. Additional information about the complimentary credit monitoring services are on the next page.

For More Information:

We sincerely regret any inconvenience that this matter may cause you and remain dedicated to maintaining the security and protection of your information. We encourage you to remain vigilant and review the enclosed addendum outlining additional steps you can take to protect your personal information. If you have questions, please do not hesitate to call 800-387-6320, Monday – Friday, 9:00 a.m. to 9:00 p.m., ET.

Sincerely,

Ricky Spike

Ricky Spike, CPA
Partner



Activation Code: <<Activation Code>>

Complimentary One-Year myTrueIdentity Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (myTrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the myTrueIdentity website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the six-digit telephone passcode <<Insert static 6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

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 Arizona, Colorado, Maryland, Rhode Island, Illinois, New York, and North Carolina:

You can obtain information from the 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>

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000
www.coag.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Illinois Office of the Attorney General Consumer Protection Division 100 W Randolph St., Chicago, IL 60601 1-800-243-0618
www.illinoisattorneygeneral.gov

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
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
888-397-3742

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

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