July 8, 2020

Anjali Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

VIA EMAIL DOJ-CPB@doj.nh.gov;
Attorneygeneral@doj.nh.gov

Attorney General Gordon McDonald
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03302
DOJ-CPB@doj.nh.gov

Re: Data Security Incident

Dear Attorney General McDonald:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Eshel, Aminov & Partners LLP ("Eshel Aminov"), an accounting and financial services firm, with respect to a potential data security incident (hereinafter, the "Incident") described in more detail below. Eshel Aminov takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

1. Nature of the security Incident.

Beginning on or about March 10, 2019 and ending on or about May 20, 2019, Eshel Aminov experienced a business email compromise in which an unknown cyber attacker gained access to Eshel Aminov's business email environment as a result of an email phishing scheme.

Eshel Aminov does not know what, if any, personal information belonging to its clients was either acquired or accessed by the unknown cyber attacker as a result of this Incident. However, the individual responsible for the Incident had the means to access and/or acquire unencrypted documents within Eshel Aminov's business email environment that contained Social Security numbers, financial information, payment card information, and tax-related information of Eshel Aminov's clients.

Again, at this time, Eshel Aminov has no evidence that the cyber attacker actually viewed or acquired any personal information or that any fraud of misuse of any personal information has occurred due to the Incident.

Eshel Aminov first discovered the Incident on or about May 10, 2019, at which time it swiftly took steps to secure its business email environment. Eshel Aminov has since gone to great lengths to identify and notify any individuals who were potentially impacted as result of this incident including (1) a thorough internal review of tens of thousands of client files (2) the hiring of a third-party vendor to organize and process Eshel Aminov client mailing data and (3) the hiring of a third-party vendor to arrange for any potentially affected individuals to receive credit monitoring and identify theft protection services.

2. Number of New Hampshire residents affected.

On or about April 15, 2020, Eshel Aminov finished identifying a population of six (6) New Hampshire residents that were potentially affected by this Incident. Incident notification letters addressed to these individuals were mailed on July 8, 2020, via First Class Mail. A sample copy of the two versions[1] of the Incident notification letters being mailed to potentially affected residents of New Hampshire are included with this letter.

3. Steps taken.

Eshel Aminov has taken steps to prevent a similar event from occurring in the future. These steps include resetting Eshel Aminov employees' access credentials through a "global" firm-wide password reset, implementing additional layers of security to Eshel Aminov's email platform, and reviewing the ways confidential information is transmitted within the firm. Additionally, Eshel established a new "client portal" for secure transfer of data. Eshel Aminov has also provided potentially impacted individuals with notice of the Incident and complimentary, online credit monitoring and identity theft protection services to all notified residents of New Hampshire for twelve (12) months.

4. Contact information.

Eshel Aminov remains dedicated to protecting the sensitive information within 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

[1] Both versions of the incident notification letters are being mailed on July 8, 2020. The letter being sent to "primary clients," heads of household and their spouses, is at **Exhibit A**. The letter being sent to "dependents" of Eshel Aminov's primary clients is at **Exhibit B**.

WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

EXHIBIT A

EMCA

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

6018000997524
000 0000001 00000000 0001 0004 00023 INS:
[redacted]

July 1, 2019

Dear [redacted]:

We are writing to inform you of an incident that may have resulted in the disclosure of your personal information. We take the security of all personal information maintained by our firm very seriously, and we sincerely apologize for any inconvenience this incident may cause.

Eshel, Aminov & Partners LLP was the victim of a business email compromise incident during which a cyber attacker gained access, without our permission, to the confidential business email accounts of our employees as a result of an email phishing scheme.

Our investigation of this cyber incident has determined that the individual(s) responsible for the cyber incident had the means to access and/or acquire documents that may have contained your Social Security number, financial and payment card numbers (including any access codes or PINs associated with those numbers) and tax-related information.

However, we are not aware of any evidence that the cyber attacker actually viewed or acquired any personal information, nor are we aware of any evidence to believe that any fraud or misuse of any personal information whatsoever has occurred as a result of this incident. Nevertheless, we wanted to send you this letter to provide you with resources to help you protect your information.

On or about May 20, 2019 our internal investigation of this incident revealed to us that the incident began on or about March 10, 2019 and ended on or about May 20, 2019. We have had the utmost privilege of serving many clients over the years, and, as such, it has been challenging to notify thousands of past and former clients of this incident all at once. To that end, our efforts have included, among other endeavors (1) expending significant internal resources during the latter half of 2019 in compiling and centralizing information related to individuals who may have been affected by this incident, (2) hiring an outside vendor in early 2020 to examine these records and to extract and process the information needed to properly deliver this notification letter to you, and (3) arranging for the provision of complimentary services, described below, that we are providing to you to help protect your personal information.

We sincerely regret any inconvenience that this incident may cause and can assure you that we have taken steps to prevent a similar event from occurring in the future. This includes resetting employees' access credentials to ensure our systems are secure, implementing additional layers of security to our email platform, and reviewing the way that confidential information is transmitted within the firm. Additionally, in 2019, we established a new "client portal" for the secure transfer of data. This portal may be accessed via our website: https://www.eshelcpa.com/.

As a safeguard, we have arranged for you to enroll in a complimentary, online credit monitoring service (*my*TrueIdentity) for 12 months provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

To enroll in this service, go to the *my*TrueIdentity website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code [redacted] and follow the three steps to receive the 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 [redacted] 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 October 31, 2020. 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.

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.)

Eshel, Aminov & Partners LLP remains dedicated to protecting your personal information. Should you have any questions or concerns about this incident, please contact 866-977-0780, Monday through Friday from 9 am to 9 pm EST for more information.

Sincerely,

Tariel Aminov, CPA
Managing Partner
Eshel, Aminov & Partners 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.gov

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 the Attorney General
Bureau of Consumer Frauds & Protection
The Capitol
Albany, NY 12224-0341
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
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.

WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

EXHIBIT B

EMCA

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

6018001007570
000 0000001 00000000 0001 0004 00008 INS:
To Parent, Guardian, or Household Member of
[redacted]

July 8, 2020

Dear Parent, Guardian, or Household Member of [redacted]:

We are writing to inform you of an incident that may have resulted in the disclosure of [redacted]'s personal information. We take the security of all personal information maintained by our firm very seriously, and we sincerely apologize for any inconvenience this incident may cause.

Eshel, Aminov & Partners LLP was the victim of a business email compromise incident during which a cyber attacker gained access, without our permission, to the confidential business email accounts of our employees as a result of an email phishing scheme.

Our investigation of this cyber incident has determined that the individual(s) responsible for the cyber incident had the means to access and/or acquire documents that may have contained [redacted]'s Social Security number, financial and payment card numbers (including any access codes or PINs associated with those numbers) and tax-related information.

However, we are not aware of any evidence that the cyber attacker actually viewed or acquired any personal information, nor are we aware of any evidence to believe that any fraud or misuse of any personal information whatsoever has occurred as a result of this incident. Nevertheless, we wanted to send you this letter to provide you with resources to help you protect [redacted].

On or about May 20, 2019 our internal investigation of this incident revealed to us that the incident began on or about March 10, 2019 and ended on or about May 20, 2019. We have had the utmost privilege of serving many clients over the years, and, as such, it has been challenging to notify thousands of past and former clients of this incident all at once. To that end, our efforts to address this incident have included, among other endeavors (1) expending significant internal resources during the latter half of 2019 in compiling and centralizing information related to individuals who may have been affected by this incident, (2) hiring an outside vendor in early 2020 to examine these records and to extract and process the information needed to properly deliver this notification letter to you, and (3) arranging for the provision of complimentary services, described below, that we are providing to you to help protect your personal information.

We sincerely regret any inconvenience that this incident may cause and can assure you that we have taken steps to prevent a similar event from occurring in the future. This includes resetting employees' access credentials to ensure our systems are secure, implementing additional layers of security to our email platform, and reviewing the way that confidential information is transmitted within the firm. Additionally, in 2019, we established a new "client portal" for the secure transfer of data. This portal may be accessed via our website: https://www.eshelcpa.com/.

As a safeguard, we have arranged for [redacted] to enroll in a complimentary, online credit monitoring service (*my*TrueIdentity) for 12 months provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

To enroll in this service, go to the *my*TrueIdentity website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code [redacted] and follow the three steps to receive the 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 [redacted] 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 October 31, 2020. 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.

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.)

Please note, this same service may not be available to affected minors. As an alternative, you can check to see if your child may be a victim of identity theft by using TransUnion's secure online form at www.transunion.com/childidentitytheft to submit your information so TransUnion can check their database for a credit file with your child's Social Security Number. After TransUnion's search is complete, they will respond to you at the email address you provide. If they locate a file in your child's name, they will ask you for additional information in order to proceed with steps to protect your child from any impact associated with this fraudulent activity.

Eshel, Aminov & Partners LLP remains dedicated to protecting your personal information. Should you have any questions or concerns about this incident, please contact 866-977-0780, Monday through Friday from 9 am to 9 pm EST for more information.

Sincerely,

Tariel Aminov, CPA
Managing Partner
Eshel, Aminov & Partners 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.gov

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 the Attorney General
Bureau of Consumer Frauds & Protection
The Capitol
Albany, NY 12224-0341
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
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.