WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

April 15, 2021

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

Kate A. Jarrett
313.327.3127 (direct)
Kate.Jarrett@wilsonelser.com

Via First Class Mail

Attorney General Gordon J. MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: February 2021 Cybersecurity Incident
Client: Schiller DuCanto & Fleck, LLP
File No.: 15991.00932

Dear Attorney General MacDonald:

We represent Schiller DuCanto & Fleck, LLP ("SDF Law") a law firm located in Chicago, IL regard to a recent cybersecurity incident. SDF Law takes this matter very seriously and is taking measures to remediate the incident and provide notice to potentially affected individuals.

1. **Nature of the incident.**

On or around February 26, 2021, SDF Law discovered a potential security issue with some of its computer systems that may have resulted in the exposure of personally identifiable information ("PII"). SDF Law immediately took the affected systems offline and engaged third-party experts to conduct a forensic investigation that disclosed that there was a cybersecurity attack.

The forensic investigation revealed that those who instigated the cybersecurity attack gained access to systems containing client information. Forensics also discovered that a small portion of client files that include personally identifiable information ("PII") were exfiltrated and potentially made public by the unauthorized individuals. PII impacted includes client names in combination with one or more of the following: date of birth, financial information and / or Social Security number.

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

SDF Law discovered that one (1) resident of New Hampshire was impacted by this incident. Notification letters were sent to these individuals between April 13, 2021 and April 15, 2021. A sample notice letter that was sent to each impacted individual is included as **Exhibit A**.

3. Steps taken.

SDF Law is committed to taking action as needed to address the situation and to help ensure that a similar situation does not occur in the future. SDF Law has also provided credit monitoring to the clients whose PII was potentially accessed and made public by an unauthorized individual.

4. Contact information.

SDF Law 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

EXHIBIT A

SCHILLER DuCANTO & FLECK LLP

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear: <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Schiller DuCanto and Fleck LLP ("SDF Law") recently experienced a sophisticated cybersecurity attack that caused a disruption to some of our computer servers. In addressing the disruption, we immediately took affected systems offline, notified law enforcement and engaged third-party experts to help investigate the full scope of the matter. Our systems are now fully restored, and we anticipate no further delays moving forward. We write to you now to inform you of the results of the investigation including what we do and do not know and steps we want to take to help protect you.

Our records indicate that some of your personal data was on our systems in connection with a current or former legal matter being handled by our firm. This letter contains additional information about the incident and steps you can take to help protect your information.

What Happened?

On or around February 26, 2021, SDF Law discovered a potential security issue with some of its computer systems that may have resulted in the exposure of your personal data. SDF Law immediately took the affected systems offline and engaged third-party experts to conduct a forensic investigation that disclosed that there was a cybersecurity attack.

What Information was Involved?

The forensic investigation revealed that those who instigated the cybersecurity attack gained access to some client files that include your personally identifiable information ("PII") that were on the impacted system. Specifically, your name in combination with one or more of the following may have been viewed by an unauthorized individual: date of birth, financial information and / or Social Security number. As such, we are notifying you of this incident out of an abundance of caution and not because we know with certainty that the unauthorized individuals misused your personal information.

What we are doing and what can you do:

SDF Law continues to take the security of your information very seriously. In order to help relieve concerns following this incident, we have secured the services of Kroll to provide identity monitoring services, at no cost to you, for 12 months.

Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

You have until **July 13, 2021** *to activate your identity monitoring services.*

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

We cannot tell you how deeply sorry we are for any anxiety and inconvenience this incident may have caused. Information security is a top priority to us, and we are committed to taking action as needed to address the situation and to help ensure that a similar situation does not occur in the future.

We encourage you to remain vigilant and review the enclosed addendum outlining additional steps you can take to help protect your personal information. If you have any questions, please call 1-855-723-1668, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding some U.S. holidays. Please have your membership number ready.

Sincerely,

Meighan A. Harmon
Managing Partner
Schiller DuCanto & Fleck 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 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
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

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.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

SCHILLER DUCANTO & FLECK LLP

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear: <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Schiller DuCanto & Fleck LLP ("SDF Law") recently experienced a sophisticated cybersecurity attack that caused disruption to some of our computer servers. We immediately took affected systems offline, notified law enforcement and engaged third-party experts to investigate the full scope of the matter. Our systems are now fully restored, and we anticipate no further delays moving forward. As a result of the foregoing investigation, our experts have not found evidence that your personal information was compromised. Never-the-less, we write to you now to inform you of the results of the investigation including what we do and do not know and steps we want to take to help protect you.

Our records indicate that personal data of yours was in our system in connection with a current or former legal matter handled by our firm.

What Happened?

On or around February 26, 2021, SDF Law discovered a potential security issue with some of its computer systems. SDF Law immediately took the affected systems offline and engaged third-party experts to conduct a forensic investigation that disclosed that there was a cybersecurity attack.

What Information was Involved?

The forensic investigation was unable to determine whether those that instigated the cybersecurity attack gained access to your personally identifiable information ("PII") stored on the impacted system. As such, we are notifying you of this incident out of an abundance of caution. As previously stated, SDF Law does not have any evidence that your PII was accessed.

What we are doing and what can you do:

SDF Law continues to take the security of your information very seriously. We cannot tell you how deeply sorry we are for any anxiety and inconvenience this incident may have caused you, and we appreciate your patience and support as we restored our systems. Information security continues to be a top priority for the firm, and we are committed to taking action as needed to address the situation and to help ensure that a similar situation does not occur in the future.

If you have any questions, please call 1-855-723-1668, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding some U.S. holidays.

Sincerely,

Meighan A. Harmon
Managing Partner
Schiller DuCanto & Fleck 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 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
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

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.