



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Samuel Sica, III
Office: (267) 930-4802
Fax: (267) 930-4771
Email: ssica@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

January 7, 2021

VIA E-MAIL

Office of the Attorney General
Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Sherin and Lodgen LLP (“Sherin and Lodgen”) located at 101 Federal Street, Boston, MA 02110 and are writing to notify your office of an event that may affect the security of certain personal information relating to approximately three (3) Maryland residents. This notice may be supplemented with new significant facts learned subsequent to its submission. By providing this notice, Sherin and Lodgen does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On June 6, 2021, Sherin and Lodgen was alerted to issues related to the functionality of its email system. Sherin and Lodgen, through its third-party IT providers, immediately began investigating the source of the disruption. A preliminary investigation identified potential unauthorized access. Sherin and Lodgen engaged third-party incident response specialists, including network security specialists and forensic investigation firm, to assess the security of its systems and confirm the nature and scope of the event. Through the investigation, it was determined that an unauthorized actor had access to certain Sherin and Lodgen systems between June 2, 2021 and June 6, 2021. On or about June 12, 2021, the forensic investigation revealed that the unauthorized actor had gained access to and acquired certain files from within the Sherin and Lodgen system.

Sherin and Lodgen, with the assistance of third-party document review specialists, promptly conducted a comprehensive programmatic and manual review of the identified files to determine whether personal information was contained therein and to whom that information related. Sherin and Lodgen also performed time-intensive review of its internal records to locate contact information for the identified individuals to provide notice of the data event. On or about November 4, 2021, Sherin and Lodgen identified personal

information relating to certain individuals was contained in one or more of the involved files. Sherin and Lodgen then undertook a review of its records to identify contact information associated with the potentially affected individuals. There is presently no indication that personal information has been disclosed publicly or used for any fraudulent purpose as a result of this event.

The information that may have been subject to unauthorized access for Maryland residents includes name and Social Security Number.

Notice to Maryland Residents

On or about January 7, 2021, Sherin and Lodgen provided written notice of this event to affected individuals known to date, which includes approximately three (3) Maryland residents. Written notice is being provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Sherin and Lodgen moved quickly to investigate and respond to the event, assess the security of its systems, inform the Federal Bureau of Investigation, and notify potentially affected individuals. In coordination with third-party digital forensic specialists, Sherin and Lodgen reviewed and enhanced the existing security measures related to the network, isolated and terminated suspicious activity identified on the potentially affected systems, and conducted a thorough forensic analysis of these systems. Sherin and Lodgen also confirmed that patching and updating was current within the network, reset all passwords, and confirmed that multi-factor authentication was appropriately implemented.

Sherin and Lodgen is providing access to credit monitoring and identity restoration services for 12 months, through Equifax, to individuals whose personal information was potentially affected by this event, at no cost to these individuals. Additionally, Sherin and Lodgen is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Sherin and Lodgen is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4802.

Very truly yours,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/arf
Enclosure

EXHIBIT A



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>>

NOTICE OF <<VARIABLE HEADER>>

Dear <<Name 1>>:

Sherin and Lodgen LLP ("Sherin and Lodgen") is writing to inform you of an event that could affect the security of some of your information. This notice provides information about the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? On June 6, 2021, our IT Support received a report of issues related to the functionality of our email system. We immediately began investigating this report and through that investigation identified potential unauthorized access on certain Sherin and Lodgen systems. That same day we engaged cyber incident response specialists, including a leading third-party forensic investigation firm, to assess the security of our systems and to confirm the nature and scope of the event. Our investigation confirmed that an unauthorized actor had access to certain Sherin and Lodgen systems between June 2, 2021 and June 6, 2021. It was further determined that certain Sherin and Lodgen files were accessed or acquired by the unauthorized actor during that timeframe. We identified these files and conducted a thorough review of each file to identify whether personal information was contained therein and to whom that information related. As a result of this in-depth review, on or about November 4, 2021, we determined that some of your personal information was contained in one or more of the involved files.

What Information Was Involved? Our investigation determined that at the time of the event the involved files contained information including your name, <<Data elements/VARIABLE TEXT 2>>.

What We Are Doing. Safeguarding the privacy of information held in our care and the security of our network is among our firm's highest priorities. Sherin and Lodgen has strict security measures in place to protect information in our care. Upon learning of this event, we immediately shut down impacted systems, reset passwords for all Sherin and Lodgen users, notified law enforcement, and brought in third-party specialists to investigate and remediate the matter. We also took action to further enhance our security measures already in place to protect our network systems and data.

As an added precaution, we are offering you access to <<12/24>> months of credit monitoring and identity restoration services through Equifax at no cost to you. More information about these services and instructions on how to enroll are enclosed with this letter.

What You Can Do. At this time, there is no indication that your information has been disclosed publicly or used for any fraudulent purpose as a result of this event; however, we encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may also enroll to receive the free credit monitoring and identity restoration services we are offering and review the enclosed “Steps You Can Take to Protect Your Information” to learn more about ways to protect personal information.

For More Information. If you have additional questions, you may contact 855-604-1738, Monday through Friday, 9 a.m. to 9 p.m., Eastern Time. You may also write to Sherin and Lodgen at 101 Federal Street, Boston, MA 02110.

We continue to devote significant resources to protect and maintain the confidentiality of information entrusted to us and regret any inconvenience or concern this notification may cause you.

Sincerely,

Sara Jane Shanahan
Managing Partner
Sherin and Lodgen LLP

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring



Enter your Activation Code: <<Activation Code>>

Enrollment Deadline: <<Enrollment Deadline>>

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of <<Activation Code>> then click "Submit" and follow these 4 steps:

1. **Register:**

Complete the form with your contact information and click "Continue".

If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click 'Sign Me Up' to finish enrolling.

You're done!

The confirmation page shows your completed enrollment.

Click "View My Product" to access the product features.

To sign up for US Mail delivery, dial 1-855-833-9162 for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.

1. Activation Code: You will be asked to enter your enrollment code as provided at the top of this letter.

2. Customer Information: You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.

3. Permissible Purpose: You will be asked to provide Equifax with your permission to access your Equifax credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment.

4. Order Confirmation: Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.

¹WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. ²The Automatic Fraud Alert feature is made available to consumers by Equifax

Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. ³Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax

*Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com ⁴The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions. *

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street NW, Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 17 Rhode Island residents impacted by this incident.