



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Gregory J. Bautista
Office: (267) 930-1509
Fax: (267) 930-4771
Email: gbautista@mullen.law

1266 E. Main Street, Soundview Plaza,
Suite 700 R
Stamford, CT 06902

February 14, 2024

VIA E-MAIL

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

Re: Notice of Data Event

To Whom It May Concern:

We represent Naulty, Scaricamazza & McDevitt, LLC (“NSM”) located at One Penn Center, Suite 750, 1617 JFK Boulevard, Philadelphia, PA 19103, and are writing to notify your office of an incident that may affect the security of certain personal information relating to sixteen (16) Maryland residents. By providing this notice, NSM 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 October 16, 2022, NSM identified suspicious activity on their network. NSM immediately took steps to secure its network, and launched an investigation, with the assistance of third-party forensic specialists to determine the nature and scope of the activity. Through the investigation, NSM determined that an unknown actor gained access to certain systems between October 11, 2022 and October 16, 2022. As a result, the unauthorized actor may have had access to certain files within these systems and information may have been accessed or acquired by the unauthorized actor during this incident. Accordingly, NSM quickly began a diligent and comprehensive review to identify sensitive information that may have been contained within the impacted systems and to identify the individuals whose information may have been present. The information that could have been subject to unauthorized access includes name, driver’s license number, Social Security number, individual health insurance policy number, and medical condition or treatment information.

Notice to Maryland Residents

On February 5, 2024, NSM completed its most recent review and address enrichment efforts. On February 14, 2024, NSM provided written notice of this incident to sixteen (16) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, NSM moved quickly to investigate and respond to the incident, assess the security of NSM systems, and identify potentially affected individuals. Further, NSM notified federal law enforcement regarding the event. NSM is also working to implement additional safeguards and training to its employees. NSM is providing access to credit monitoring services for twelve (12) months, through Epiq, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

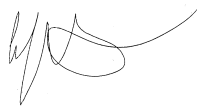
Additionally, NSM is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. NSM is providing individuals with information 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.

NSM is providing written notice of this incident to relevant state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1509.

Very truly yours,



Gregory J. Bautista of
MULLEN COUGHLIN LLC

GJB/kzf
Enclosure

EXHIBIT A



NAULTY, SCARICAMAZZA & McDEVITT, LLC

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 DATA <<VARIABLE HEADER>>

Dear <<Name 1>>:

Naulty, Scaricamazza & McDevitt, LLC (“NSM”) writes to inform you of a recent event that may impact the privacy of some of your information. We are unaware of any attempted or actual misuse of your information at this time, but we are providing you with this letter as a precaution, to inform you of the event, our response, and steps you may take to protect your information, should you feel it is necessary to do so.

What Happened? On October 16, 2022, NSM identified suspicious activity on our network. We immediately took steps to secure our network, and launched an investigation, with the assistance of third-party forensic specialists to determine the nature and scope of the activity. Through the investigation, we determined that an unknown actor gained access to certain systems between October 11, 2022 and October 16, 2022. As a result, the unauthorized actor may have had access to certain files within these systems and information may have been accessed or acquired by the unauthorized actor during this incident. As a result, NSM quickly began a diligent and comprehensive review to identify sensitive information that may have been contained within the impacted systems and to identify the individuals whose information may have been present. We are notifying you now because the process is complete and the investigation determined certain information related to you may have been impacted.

What Information Was Involved? This information includes your <<Data Elements>>, and your name. While we have no indication that your information was subject to actual or attempted misuse as a result of this incident, we are notifying you out of an abundance of caution.

What We Are Doing. We take this incident and the security of your information seriously. Upon discovery, NSM promptly took steps to confirm the security of our systems and commenced an investigation with the assistance of third-party computer forensics specialists. As part of our ongoing commitment to the privacy of information in our care, we are reviewing our policies, procedures, and processes related to the storage and access of sensitive information, and additional workforce training is being conducted to reduce the likelihood of a similar future event. We are also notifying applicable regulatory authorities, as required by law.

As an added precaution, we are also offering <<CM Length>> months of complimentary access to credit monitoring services through Equifax. Individuals who wish to receive these services must enroll by following the attached enrollment instructions.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and credit reports for suspicious activity and to detect errors. You can review the enclosed *Steps You Can Take to Help Protect Your Personal Information* to learn helpful tips on steps you can take to protect against possible information misuse, should you feel it appropriate to do so.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance, please contact us at 855-579-0791, Monday through Friday, between 9:00 a.m. and 9:00 p.m., Eastern Time.

NSM sincerely regrets any inconvenience or concern this incident has caused.

Sincerely,

Naulty, Scaricamazza & McDevitt, LLC

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in Credit Monitoring



<<Name1>>
Enter your Activation Code: <<ACTIVATIONCODE>>
Enrollment Deadline: <<ENROLLMENTDEADLINE>>

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 <<ACTIVATIONCODE>>, 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.

¹ WebScan 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.

² The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

³ Locking 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.

⁴ The 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	800-916-8800
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, DC 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, DC 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 <https://www.marylandattorneygeneral.gov/>. NSM is located at One Penn Center, Suite 750 1617 JFK Boulevard, Philadelphia, PA 19103.

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.