



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Kevin Dolan
Office: (267) 930-4861
Fax: (267) 930-4771
Email: kdolan@mullen.law

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

July 5, 2023

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 Smyser Kaplan & Veselka (“SKV”) located at 717 Texas Ave # 2800, Houston, TX 77002, and are writing to notify your office of an incident that may affect the security of certain personal information relating to twenty nine (29) Maryland residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, SKV 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

In September 2022, SKV detected suspicious activity on certain systems within its network. Upon learning of this activity, SKV took immediate steps to confirm their systems’ security and initiated a comprehensive investigation with assistance from external computer forensic specialists. SKV worked diligently to investigate this activity and to confirm its impact on its systems, including identifying the risk to any data present within the network. The investigation confirmed an unauthorized actor accessed specific network locations and acquired documents from the network on or around September 26, 2022. SKV initiated an exhaustive and time-intensive manual data review process to identify the specific information potentially impacted and corresponding individuals. This comprehensive review was completed on April 11, 2023, and SKV is notifying potentially impacted individuals.

The information that could have been subject to unauthorized access includes name, Social Security number, health insurance information, medical information, and financial account information.

Notice to Maryland Residents

On or about July 5, 2023, SKV began providing written notice of this incident to approximately twenty nine (29) 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, SKV moved quickly to investigate and respond to the incident, assess the security of SKV systems, and identify potentially affected individuals. Further, SKV notified federal law enforcement regarding the event. SKV is also working to implement additional safeguards and training to its employees. SKV is providing access to credit monitoring services for one (1) year, through Equifax to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, SKV 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. SKV 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.

SKV is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4861.

Very truly yours,

Kevin Dolan of
MULLEN COUGHLIN LLC

KED/jrl
Enclosure

EXHIBIT A



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<First Name>> <<Middle Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

July 5, 2023

<<VARIABLE HEADER>>

Dear <<First Name>> <<Middle Name>> <<Last Name>>:

Smyser Kaplan & Veselka writes to notify you of a recent event that may impact the privacy of some of your information. We are providing you with information about the event, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so. We are also offering you complimentary credit monitoring services at no cost; enrollment instructions are on the following pages.

What Happened? In September 2022, SKV detected suspicious activity on certain systems within our network. Upon learning of this activity, we took immediate steps to confirm our systems' security and initiated a comprehensive investigation with assistance from external computer forensic specialists. We worked diligently to investigate this activity and to confirm its impact on our systems, including identifying the risk to any data present within our network. The investigation confirmed an unauthorized actor accessed specific network locations and acquired documents from the network on or around September 26, 2022. We initiated an exhaustive and time-intensive manual data review process to identify the specific information potentially impacted and corresponding individuals so we could alert them to the event. This comprehensive review was completed on April 11, 2023, and we are notifying you because this review determined your information may have been accessed and/or acquired by the unauthorized actor.

What Information Was Involved? We determined the impacted information may include your name and <<Breached Elements>>.

What We Are Doing. We value the privacy and security of all information in our care. Upon becoming aware of the event, we immediately initiated a comprehensive investigation that included reporting the activity to the FBI. We continue to assess our network security, including reviewing and enhancing policies and procedures as appropriate. As an added precaution, we are offering you access to <<12/24>> months of complimentary credit monitoring services. Enrollment instructions are enclosed with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports. You should immediately report any suspicious activity to law enforcement. We encourage you to review the information contained in the enclosed *Steps You Can Take To Help Protect Information* and to enroll in the complimentary monitoring services.

For More Information. We understand that you may have questions that are not addressed in this notice. If you have additional questions, please call our dedicated assistance line at 844-566-1546, which is available from 9:00 AM to 9:00 PM EST Monday through Friday (excluding major U.S. holidays).

Sincerely,

Smyser Kaplan & Veselka

STEPS YOU CAN TAKE TO HELP PROTECT INFORMATION

Enroll in Credit Monitoring



<<First Name>> <<Last Name>>

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.

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 credit 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	1-800-916-8800
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 www.marylandattorneygeneral.gov/. SKV is located at 717 Texas Avenue, #2800, Houston, TX 77002.

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 www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., 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 approximately <<RI Count>> Rhode Island residents impacted by this incident.