MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Ryan C. Loughlin
Office: (267) 930-4786
Fax: (267) 930-4771
Email: rloughlin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

July 26, 2018

VIA U.S. 1st CLASS MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General MacDonald:

We represent SVAM International, Inc. ("SVAM"), 233 East Shore Road, Great Neck, New York, 11023, and are writing to notify your office of an incident that may affect the security of personal information relating to one (1) New Hampshire resident. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, SVAM does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

On May 30, 2018, SVAM became aware of efforts by an unauthorized individual to provide several clients with fraudulent wiring instructions. SVAM immediately commenced an investigation into this activity to determine what happened and what information may be affected. This investigation included working with third party forensic investigators to confirm the nature and scope of this incident. Through the investigation, it was determined that there was unauthorized access to several employee email accounts between April 24, 2018 and May 30, 2018. It is believed that this access occurred after the employees received phishing emails. Further investigation determined that the unauthorized individual ran searches in the email accounts for terms such as "invoice," "wire," and "payment." Additionally, the investigation determined that certain emails and/or attachments may have been viewed without authorization. A review of the emails and/or attachments that may have been viewed without authorization determined that the emails may contain certain information, including name, address and Social Security number.

Notice to New Hampshire Resident

SVAM began providing written notice to potentially affected individuals, including one (1) New Hampshire resident, by mail on July 26, 2018. Written notice was provided in substantially the same form as the letter attached here as ***Exhibit A***.

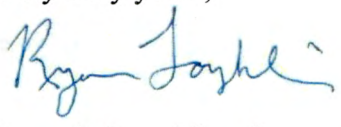
Other Steps Taken to Be Taken

Upon learning of the efforts to provide fraudulent wire transfer information, SVAM immediately commenced an investigation to confirm the nature and scope of the incident and to identify what information may be affected. SVAM also took steps to prevent further unauthorized access to the email accounts by changing passwords. While SVAM has measures in place to protect information in its systems, SVAM is reviewing its existing policies and procedures. SVAM is providing all potentially affected individuals complimentary access to twelve (12) free months of credit and identity monitoring services, including identity restoration services, through Kroll. Additionally, SVAM is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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. SVAM notified federal law enforcement and is also providing written notice of this incident to other 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 267-930-4786.

Very truly yours,



Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL:ncl
Enclosure

EXHIBIT A

SVAM INTERNATIONAL, INC.

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

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Re: Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

We write regarding a recent email phishing event that may have impacted the security of your personal information. We want to provide you with information about the incident, our response and steps you may take to better protect against possible misuse of your personal information, should you feel it necessary to do so.

What Happened? On May 30, 2018, SVAM became aware of efforts by an unauthorized individual to provide several clients with fraudulent wiring instructions. SVAM immediately commenced an investigation into this activity to determine what happened and what information may be affected. This investigation included working with third party forensic investigators to confirm the nature and scope of this incident. Through the investigation, we determined that there was unauthorized access to several employee email accounts between April 24, 2018 and May 30, 2018. It is believed that this access occurred after the employees received phishing emails. Further investigation determined that the unauthorized individual ran searches in the email accounts for terms such as "invoice," "wire," and "payment." Additionally, the investigation determined that certain emails and/or attachments may have been viewed without authorization.

What Information was Involved? A review of the emails and/or attachments that may have been viewed without authorization determined that the emails may contain certain information related to you, including your <<ClientDef1 (name, address, [insert field with specific information].)>>

What We Are Doing. The confidentiality, privacy, and security of our employee information is one of our highest priorities. Upon learning of the event, we immediately commenced an investigation to confirm the nature and scope of the incident and to identify what information may be affected. We also took steps to prevent further unauthorized access to the email accounts by changing passwords. While we have measures in place to protect information in our systems, we are reviewing our existing policies and procedures.

As an added precaution, we are offering you access to one year of credit monitoring and identity theft restoration services through Kroll at no cost to you. Please review the attached "Steps You Can Take to Protect Your Information" for information on these services and instruction on how to enroll. We encourage you to enroll in these services as we are not able to act on your behalf to do so.

What You Can Do. Please review the enclosed "Steps You Can Take to Protect Your Information," which contains information on what you can do to better protect against possible misuse of your information. You may also enroll in the credit monitoring and identity theft restoration services we are offering.

For More Information. We understand you may have questions that are not answered in this letter. If you have questions, please contact Kroll at 1-???-???-???? Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time.

Sincerely,

Marchese

Joe Marchese
Managing Director

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll Credit Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. 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, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <<IDMonitoringURL>> to activate and take advantage of your identity monitoring services.
You have until <<Date>> to activate your identity monitoring services.
Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-???-???-????. Additional information describing your services is included with this letter.

Monitor Your Accounts

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus listed below to request a free copy of your credit report.

Fraud Alerts. At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19106
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from $3 to $15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.freeze.equifax.com	www.experian.com/freeze/	www.transunion.com/credit-freeze

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General, as well as the credit reporting agencies listed above. The Federal Trade Commission can 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. For Maryland residents, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. For North Carolina residents, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice was not delayed as the result of a law enforcement investigation.

Kroll

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] 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 can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. 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.