SheppardMullin

Sheppard, Mullin, Richter & Hampton LLP
30 Rockefeller Plaza
New York, New York 10112-0015
212.653.8700 main
212.653.8701 fax
www.sheppardmullin.com

212.634.3077 direct
krollins@sheppardmullin.com

January 9, 2019

File Number: 63KM-285953

VIA ELECTRONIC MAIL

Attorney General Bob Ferguson
Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504
E-Mail: securitybreach@atg.wa.gov

Re: Notice of Data Breach

Dear Attorney General Ferguson:

We are writing on behalf of our client, A&A Global Imports Inc., to inform you of a data incident.

On August 17, 2018, A&A was notified by law enforcement that they suspected certain of A&A's information may have been compromised by unknown cyber-attackers. Upon receiving this notification, A&A coordinated with law enforcement and immediately engaged with several firms, including a leading computer forensic firm, to conduct a forensic investigation into the matter to determine whether a "breach" under Washington law had occurred, to understand the scope of the breach (if one had occurred), and to restore the integrity and security of the impacted systems.

As a result of that investigation, A&A discovered that unknown cyber-attackers had placed unauthorized code on its website that may have been capable of capturing certain information entered on the website during the checkout process. A&A's forensic investigation further revealed that the cyber-attackers also may have been able to acquire data out of A&A's customer database. Based upon A&A's investigation to date, it appears that information entered on its website may have been exposed at various points in time, including from August 15, 2017 to January 4, 2019. A&A has removed the malicious code, and increased website security in an effort to prevent incidents like this from happening again. As a further precautionary measure, A&A also migrated its website to an entirely new platform.

Based upon A&A's investigation, the information impacted may have included customer names, phone numbers, usernames, passwords, addresses, and in some instances, credit card numbers, expiration date, and CVV code. The information did not include customer Social Security Numbers, driver's license numbers, state identification numbers, health information, or any other financial information.

From A&A's investigation, it appears that the personally identifiable information 2,783 Washington residents may have been impacted. Once A&A's forensic investigation revealed a breach

impacting Washington residents, and had restored the integrity and security of the impacted systems, A&A prepared to notify to those impacted individuals. Notifications to the impacted individuals in Washington will be sent on or around January 9, 2019. A copy of the notice is enclosed.

Even though A&A has no evidence that any personal information has been fraudulently used as a result of this incident, out of an abundance of caution, A&A is offering impacted individuals 12 months of free credit monitoring and identity theft protection through Experian's IdentityWorks program. Additionally, in its written notification, A&A has provided potentially impacted individuals with detailed information regarding additional steps they can take to protect themselves and their personal information.

We assure you that our client, A&A, takes this issue, and the privacy and security of its customers, very seriously. If you have any questions or require further information, please feel free to contact me at krollins@sheppardmullin.com or (212) 634-3077.

Sincerely,

Kari M. Rollins
for SHEPPARD, MULLIN, RICHTER & HAMPTON LLP

SMRH:488861705.1
Enclosure

Return Mail Processing Center
PO 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>>

Dear <<Name1>>:

I am writing to inform you of an incident that may have impacted some of your personal information. A&A Global Imports values its customers' privacy, and sincerely regrets any inconvenience this incident may cause. We are sending you this notice to explain what happened, what information was affected, what measures we have taken, and some steps you can take in response to the incident.

What Happened?

On August 17, 2018, we were notified by law enforcement that they suspected certain of A&A's information may have been compromised by unknown cyber attackers. Upon receiving this notification, we immediately engaged with several firms, including a leading computer forensic firm, to conduct a forensic investigation into the matter. As a result of that investigation, we discovered that unauthorized code was placed on our website that may have been capable of capturing certain information entered on the website during the checkout process. Our forensic investigation further revealed that the cyber attackers also may have been able to acquire data out of our customer database. Based on our investigation to date, it appears that information entered on our website may have been exposed at various points in time, including from August 15, 2017 to January 4, 2019. Importantly, the unauthorized code identified during our forensic investigation has been removed.

What Information Was Involved?

The information that was involved may have included your name, phone number, username, password, address, and, in some instances, credit card number, expiration date, and CVV code. The information did not include your Social Security Number, driver's license number, state identification number, health information, or any other financial information.

What Are We Doing?

Upon learning about the incident, we coordinated with law enforcement and worked with a leading computer security and forensic firm to investigate the incident. We have removed the identified unauthorized code from the website and have worked to strengthen our website security to prevent this type of incident from happening in the future. We also migrated our website to an entirely new platform. While law enforcement was involved, this notice was not delayed at the request of a law enforcement agency or as a result of a law enforcement investigation.

Free fraud detection and identity theft protection. Though we have no evidence to suggest your personal information has been misused, as a precautionary measure, we have arranged for you to receive **12 months** of **free** fraud detection and identity theft protection through Experian's IdentityWorks program. This service includes identity restoration services to help you address fraud, a free credit report, active credit monitoring to detect suspicious activity, and a $1 million identity theft insurance policy, including coverage of unauthorized electronic fund transfers from your bank account.

To offer added protection, you will receive IdentityWorks ExtendCARE, which will provide you with fraud resolution support even after your IdentityWorks membership has expired. With ExtendCARE you will have access to a dedicated Identity Restoration agent who will walk you through the process of fraud resolution from start to finish. This specialist will also investigate each incident of fraud, help you in contacting credit grantors to dispute charges and close accounts, and assist you with freezing credit files (if desired).

Again, this protection is being offered at **no cost** to you for 12 months. To take advantage of these free services, you can enroll by calling Experian at (877) 890-9332 or visiting their website at www.experianidworks.com/credit, and providing them with the following **Activation Code** <<Enrollment Code>>. You have until <<Enrollment Deadline>> to register and enroll. If you have questions or need assistance with enrolling, please call (877) 890-9332 and provide the following **Engagement** #: <<Engagement Number>>. Enrolling in this service does not affect your credit score.

What You Can Do

Again, we take very seriously the security and privacy of your information, and want to make sure you have the information you need so that you can take steps to help protect your personal information. At the end of this letter, we have provided you with additional information regarding steps you can take to further protect yourself and your information. We encourage you review that additional information.

For More Information

A&A Global has setup a dedicated call center to answer questions regarding this incident. If you have any questions about the incident or this notice please call 888-724-0248 between 6:00 a.m. and 6:00 p.m. Pacific Time, Monday through Friday.

We deeply regret the inconvenience or concern that this incident might cause you.

Sincerely,

David Aryan
Chief Executive Officer

Additional Steps You Can Take To Protect Yourself

As always, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained.

You may want to contact the three U.S. credit reporting agencies to report the incident and request a credit report:

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 4500	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(866) 349-5191	(888) 397-3742	(888) 909-8872
www.equifax.com	www.experian.com	www.transunion.com

Credit Report: You can request a free credit report once a year at www.annualcreditreport.com, calling 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348.

Fraud Alert: To protect yourself from possible identity theft you can place a fraud alert on your credit file. A fraud alert informs creditors to follow certain procedures before establishing any accounts in your name. It may also delay your ability to obtain credit. You may place a fraud alert on your file by contacting the consumer reporting agencies listed above. To place an alert you may be asked to provide the consumer reporting agency with information that identifies you, including your Social Security number.

Security Freeze: In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, loan, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze on your file you may be required to provide the consumer reporting agency with information that identifies you including your Social Security Number. To put a security freeze on your credit file contact the consumer reporting agencies listed above.

If you suspect any identity theft has occurred, you may contact the Federal Trade Commission by calling (877) 438-4338 or online at www.ftc.gov. The FTC is located at 600 Pennsylvania Avenue, NW Washington, DC 20580. You can also contact local law enforcement or the attorney general in your state.

Maryland residents may wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.oag.state.md.us/idtheft, or by sending an email to idtheft@oag.statemd.us, or calling 410-576-6491.

North Carolina residents may wish to review information provided by the North Carolina Attorney General at http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699.

Rhode Island resident may wish to review information provided by the Rhode Island Attorney General at http://www.riag.ri.gov, by calling 401-274-4400, or writing to 150 South Main Street, Providence, RI 02903.