Serrin A. Turner
Direct Dial: (212) 906-1330
serrin.turner@lw.com

53rd at Third
885 Third Avenue
New York, New York 10022-4834
Tel: +1.212.906.1200 Fax: +1.212.751.4864
www.lw.com

LATHAM & WATKINS LLP

July 19, 2016

VIA EMAIL

Attorney General Bob Ferguson
Office of the Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, Washington 98504-0100
SecurityBreach@atg.wa.gov

Dear Attorney General Ferguson:

I am writing on behalf of my client, San Antonio Shoemakers, Inc. ("SAS"), to notify you that SAS recently became aware of a computer intrusion that affected checkout systems at a number of its retail stores in the United States and its customer service center which accepts telephone orders.

While SAS continues to investigate the incident, it has been determined that the checkout systems used by a number of its retail stores and its customer service center were infected with malware enabling unauthorized parties to access payment card data of some of SAS's customers. The malware attack potentially put at risk payment cards used in purchases made at certain SAS retail stores and through its customer service center between the dates of April 21, 2016—the earliest date when the malware was installed on any system—and June 13, 2016—by which time the malware was removed from all affected systems. The malware was designed to collect certain payment card information, including cardholder name, payment card number, security code and expiration date. There is no evidence that other customer information, such as contact information, Social Security numbers (which SAS never collects) or PINs, was affected by this issue.

SAS first discovered the attack on or about June 8, 2016. SAS engaged outside cybersecurity experts to conduct an extensive investigation, and the company has also been working closely with law enforcement authorities to determine the facts. Upon the written request of the United States Attorney's Office for the Southern District of New York and the New York Electronic Crimes Task Force of the United States Secret Service, SAS delayed notifying individuals potentially affected by this incident for 30 days while law enforcement began their investigation (a copy of the request is enclosed). SAS has taken steps to secure their systems and ensure that the malware no longer presents a threat to customers using payment cards at its stores.

SAS is notifying residents of Washington potentially affected by the attack for whom the company has contact information. There are at least 511 residents of Washington whose payment card information was put at risk by the attack. In addition to information about the breach, the notice will provide contact information should the individual have questions about the incident, free identity theft monitoring as offered by AllClearID, and resources and guidance for dealing with identity theft. A copy of the planned notice is attached.

Please contact me at (212) 906-1330 or serrin.turner@lw.com in the event that you have any questions regarding this matter.

Sincerely yours,

/s/ Serrin A. Turner

Serrin A. Turner
LATHAM & WATKINS LLP

Enclosures

U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

June 17, 2016

By Electronic Mail

Serrin Turner, Esq.
Latham & Watkins LLP
885 Third Avenue
New York, NY 10022

Re: San Antonio Shoemakers, Inc. Intrusion

Dear Counsel:

As we have discussed, the United States Attorney's Office for the Southern District of New York (this "Office") has been working with the New York Electronic Crimes Task Force of the United States Secret Service ("USSS") to investigate an intrusion into a suspected breach of credit card information suffered by San Antonio Shoemakers, Inc. ("SAS").

On behalf of this Office and the USSS, I write to request that SAS delay any public disclosure of this intrusion and possible data breach for approximately 30 days until July 17, 2016, or until such time as my Office advises you that public disclosure will no longer impede the investigation, whichever is sooner, because premature disclosure could impede law enforcement's ability to investigate the matter. We may seek to renew this non-disclosure request at the end of the initial 30-day period should we determine that public disclosure would still impede the investigation at that time.

Respectfully,

PREET BHARARA
United States Attorney

By: _____
Timothy T. Howard
Assistant United States Attorney
Southern District of New York
(212) 637-2308

Cc: Special Agent Tate Jarrow, USSS

San Antonio Shoemakers®
Processing Center ● P.O. BOX 141578 ● Austin, TX 78714

00001
00001
ACD1234
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

July 18, 2016

Dear John Sample,

We recently became aware of a computer intrusion that affected checkout systems at a number of San Antonio Shoemakers stores located in the United States. Promptly after discovering the issue, we engaged outside cybersecurity experts to conduct an extensive investigation. We have been working closely with law enforcement authorities and coordinating our efforts with the payment card organizations to determine the facts. We sincerely regret any inconvenience and concern that this incident may cause. We want to assure you that protecting the security of our customers' payment card information is a top priority for San Antonio Shoemakers, and we are taking this situation very seriously, from our executive team down. In order to minimize any impact on our customers, we are providing 24 months of identity protection at no cost to you (*details provided below*).

Based on the investigation, we discovered that the checkout systems at certain retail stores were infected with a type of malicious software, or "malware," enabling unauthorized parties to access payment card data of some of our customers. We want you to know that the affected stores have taken steps to secure their systems and that the malware no longer presents a threat to customers using payment cards at our retail stores. Further, we have no indication that our online store was affected by this malware attack.

We have determined the following:

The attack put at risk payment cards used at checkout terminals at certain San Antonio Shoemakers retail stores between the dates of April 21, 2016, the earliest date when the malware was installed on any system, and June 13, 2016, by which time the malware was removed from all affected systems.

The malware was designed to collect certain payment card information, including cardholder name, payment card number, security code and expiration date.

There is no evidence that other types of customer data, such as contact information, Social Security numbers (which San Antonio Shoemakers never collects) or PINs, were affected by this issue.

You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports. If you believe your payment card may have been affected, please contact your bank or card issuer immediately. The U.S. Federal Trade Commission provides further guidance on steps you can take to protect your personal information, which you can access online at https://www.identitytheft.gov.

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months:

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-422-7189 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Identity Theft Monitoring: This service offers additional layers of protection including identity theft monitoring that delivers secure, actionable alerts to you by phone and $1 million identity theft insurance coverage. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-422-7189 using the following redemption code: Redemption Code.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

You will also find attached to this letter some steps that you can take to protect your identity. We encourage you to review these steps and take appropriate action to help prevent any misuse of your information.

If you have any questions about this incident or would like more information about these services, please call 1-855-422-7189 between 8:00 a.m. and 8:00 p.m., Central Time, Monday through Saturday (excluding national holidays).

Very truly yours,

Nancy Richardson
Chief Executive Officer
San Antonio Shoemakers

Information About Identity Theft Prevention

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland and Rhode Island: You may also obtain information about preventing and avoiding identity theft from the Attorney General of your state:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

Rhode Island Office of the Attorney General, Consumer Protection Unit
150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

For residents of Massachusetts and Rhode Island: You also have the right to obtain a police report.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes (for Residents Not of Massachusetts or Rhode Island): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each*

credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax:	P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian:	P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC:	P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts and Rhode Island Residents): You have the ability to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax:	P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian:	P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC:	P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.

AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 24 months of coverage with no enrollment required;
- No cost to you – ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for 24 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events that occurred prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements
To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period.
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company.
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require;
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft;

Coverage under AllClear Identity Repair Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation")
- Incurred by you from an Event that did not occur during your coverage period;
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity;
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur; and
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud;
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail	**Mail**	**Phone**
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077