



SCHURMAN RETAIL GROUP

Enriching lives through meaningful personal connections

Processing Center • P.O. BOX 141578 • Austin, TX 78714



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

March 21, 2017

Re: Notice of Data Breach

Dear John Sample:

I am writing to make you aware of a recent email spoofing attack that may affect the security of your personal information. We take this incident very seriously and are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

What Happened? On March 8, 2017, we discovered that our company was the victim of an email spoofing attack on January 18, 2017, by an individual pretending to be our Chief Financial Officer. A request was made from what appeared to be a legitimate Schurman Retail Group (“SRG”) email address for all 2016 SRG employee Form W-2 information. Unfortunately, copies of all 2016 employee W-2 forms were provided before we discovered that the request was fraudulent. We have been working tirelessly to investigate and to mitigate the impact of the attack since we discovered the fraudulent nature of the request.

What Information Was Involved? A file, including a copy of your IRS Tax Form W-2, was sent in response to the fraudulent email. An IRS Tax Form W-2 includes the following categories of information: (1) the employee’s name; (2) the employee’s address; (3) the employee’s Social Security number; and (4) the employee’s wage information. Other than the information contained on the IRS Tax Form W-2, no personal financial information was emailed to the external email account.

What We Are Doing. The confidentiality, privacy, and security of our employee information is one of our highest priorities. SRG has stringent security measures in place to protect the security of information in our possession. At this time, we have no evidence that the individual who sent the fraudulent email accessed our computer network or that our IT systems were otherwise compromised by this attack. In addition, as part of our ongoing commitment to the security of personal information in our care, we are working to implement additional safeguards and provide additional mandatory training to our employees on safeguarding the privacy and security of information on our systems. We have contacted the IRS and will be contacting the relevant state Attorneys General.

As a precaution for those individuals affected by this incident, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The cost of this service will be paid for by SRG. It is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you



01-02-1-00

in the credit monitoring service. Instructions on how to enroll in these services are included in the attached "Steps You Can Take to Prevent Identity Theft and Fraud."

What You Can Do. You can review the enclosed "Steps You Can Take to Prevent Identity Theft and Fraud." You can also enroll to receive the free credit monitoring and identity restoration services described above. In addition, if you have not already done so, we encourage you to file your 2016 tax return as soon as possible.

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, please call our dedicated assistance line at 1-855-550-6944 (toll free), Monday through Saturday, 6:00 a.m. to 6:00 p.m. PT.

SRG takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,



Roxanne Prahser
Chief Financial Officer
Schurman Fine Papers
dba Schurman Retail Group

STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

While we continue to investigate this incident, you may take direct action to further protect against possible identity theft or financial loss.

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 March 14, 2017 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 1-855-550-6944 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. 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 1-855-550-6944 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.

We encourage you to file your tax return as soon as possible, if you have not already done so. You can also contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your 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 directly to request a free copy of your credit report.

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
P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com



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. 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. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
<https://www.freeze.equifax.com>

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. 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. **For Rhode Island Residents:** The Rhode Island Attorney General may be contacted at: Rhode Island Attorney General's Office, 150 South Main St., Providence, RI 02903. <http://www.riag.ri.gov>. Approximately 15 Rhode Island residents may have been affected by this incident. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.