STILETTOSOLUTIONS
Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

IMPORTANT INFORMATION
PLEASE READ CAREFULLY

«mail id»
«First Name» «Last Name»
«Address1»
«Address2»
«City», «State» «Zip»

«Date»

Dear «FirstName»:

The privacy and security of your personal information is of utmost importance to STILETTO Solutions and we are continuously improving our processes and systems to ensure your information is secure. We wanted to make you aware of recent unauthorized access to STILETTO Solutions cardholder payment data, including yours.

After identifying suspicious activity within our e-Commerce server, our incident response team began to investigate the incident as soon as we learned of it. Working with our forensic investigators and IT security advisors, we have learned that certain customer credit card information might have been acquired by an unauthorized party from our STILETTO Solutions server. The compromise of our e-Commerce server occurred on September 16, 2015 and may impact the security of credit and debit cards customers used for purchases through our site, stilettosolutions.com, from November 1, 2013 through and including September 16, 2015.

We have devoted considerable time and effort to determine what exact customer information may be impacted. We have determined that the information involved in this incident includes your name, billing and shipping address, e-mail, credit or debit card number, card expiration date and CVV (3 or 4 digit code on the front or back of the card). It is also possible that your username and password you use to make purchases through stilettosolutions.com was involved. We can assure you that no debit PINs are at risk. Please be advised that credit/debit card transactions for ManilowTV and/or EventBrite are not handled by STILETTO Solutions and are, therefore, not at risk as a result of this incident. In addition, we have no indication that Starz.bz has been compromised, as it is run on a system and server independent from STILETTO Solutions.

As a precautionary step, you should always remain vigilant in reviewing your financial and credit card account statements for fraudulent or irregular activity on a regular basis. You should call your bank or card issuer if you see any suspicious transactions (from September 16, 2015 to the present). The policies of the payment card brands such as Visa, MasterCard, American Express and Discover provide that you are not liable for any unauthorized charges if you report them in a timely manner. You should also ask your bank or card issuer whether a new card should be issued to you. We also recommend changing the password you use to access stilettosolutions.com.

Your trust is a top priority for STILETTO Solutions, and we deeply regret the inconvenience this may cause. The privacy and protection of our customers' information is a matter we take very seriously and we constantly enhance our processes and systems. We have already revised our security protocols and have relocated payment card data to new server systems. STILETTO Solutions is no longer storing any payment card data locally. All customer payment card data is now securely stored by our third-party processor.

We recommend that you closely review the information provided on the following pages for additional steps that you may take to protect yourself against potential misuse of your credit and debit card information, including additional privacy safeguards information. Again, we want to stress that we regret any inconvenience or concern this incident may cause you.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at (877) 341-4603. The response line is available Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time. STILETTO Solutions values your business and we look forward to your continued patronage.

Sincerely,

Christopher C. Walters
VP/Merchandising
STILETTO Solutions

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. Placing a 90-Day Fraud Alert on Your Credit File.

You may place an initial 90-day "Fraud Alert" on your credit files. A fraud alert tells creditors to contact you personally before they open any new accounts in your name, increase the credit limit on an existing account, or provide a new card on an existing account. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

TransUnion
Consumer Fraud Division
PO Box 6790
Fullerton, CA 92834-6790
www.transunion.com
1-800-680-7289

Experian
Consumer Fraud Division
PO Box 9554
Allen, TX 75013
www.experian.com
1-888-397-3742

Equifax
Consumer Fraud Division
PO Box 740256
Atlanta, GA 30374-0256
www.equifax.com
1-800-525-6285

2. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If you are an ***IOWA*** resident, please read the following:

You may also report suspected incidents of identity theft to local law enforcement or the Iowa Attorney General:

Office of the Iowa Attorney General
Consumer Protection Division
1305 East Walnut Street
Des Moines, IA 50319
(515) 281-5164
1-888-777-4590
Fax: (515) 281-6771
www.iowaattorneygeneral.gov

If you are a ***MARYLAND*** resident, please read the following:

In addition to the FTC, the Maryland Office of the Attorney General can also be contacted to obtain information on the steps you can take to avoid identity theft:

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

If you are a ***NORTH CAROLINA*** resident, please read the following:

In addition to the FTC, the North Carolina Office of the Attorney General can also be contacted to obtain information on the steps you can take to prevent identity theft:

North Carolina Department of Justice
Office of the Attorney General
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Instances of known or suspected identity theft should also be reported to law enforcement.