

550 Bailey Avenue, Fort Worth, TX 76107



Fax

To: New York State Attorney General
 New York State Consumer Protection Board
 New York State Office of Cyber Security and
 Critical Infrastructure

From: Jeffrey J. Walker

Fax: 212-416-6003
 518-474-2474
 518-474-9090

Pages: 3 including cover

Phone: _____ **Date:** 1/26/2007

Re: Notice to Customers **CC:** _____

- Urgent** **For Review** **Please Comment** **Please Reply** **Please Recycle**

● **Comments:** Please see attached correspondence.

This transmission contains confidential information and may be legally privileged. It is intended for use only by the person(s) to whom it is directed. If you have received this facsimile in error, please notify us by telephone immediately so that we can arrange for the return of the facsimile copy of the documents to us.

If you do not receive all pages of this transmission, please call 817-339-3736.

Jeffrey J. Walker
817-339-3736
Fax: 817-339-3739
jwalker@us.bombayco.com

January 26, 2007

Fax 212-416-6003

New York State Attorney General
Assistant Attorney General in Charge
Bureau of Consumer Frauds
120 Broadway, 3rd Floor
New York, NY 10271

Fax 518-474-2474

New York State Consumer Protection Board
Security Breach Notification
5 Empire State Plaza, Suite 2101
Albany, NY 12223

Fax 518-474-9090

New York State Office of Cyber Security
and Critical Infrastructure Coordination
30 South Pearl Street, Floor P2
Albany, NY 12207


RE: Notice to Customers

Dear Sir or Madam:

Last month, a laptop computer belonging to The Bombay Company, Inc. was stolen. Bombay conducted a thorough investigation of the incident and determined that some information concerning four (4) Bombay customers who live in the State of New York was contained on the computer. Though Bombay promptly contacted the local police to investigate the theft, we do not expect the computer to be recovered or the assailant to be apprehended. All affected New York customers will receive the attached letter explaining the incident.

In our judgment, it is not clear that New York's data security notification laws require customer notice for this incident because no "security code, access code, or password" for the customers' credit card numbers was included in any of the files on the stolen computer. However, we have notified all 60 affected customers across the country, because of the value Bombay places on the trust of its customers. We are also providing this notice to the above New York agencies in order to ensure open communication in the event Bombay's affected customers in New York contact these agencies with any questions.

Sincerely,


JEFFREY J. WALKER
Assistant General Counsel

Enclosure



January 22, 2007

[CUSTOMER NAME]
[CUSTOMER ADDRESS]
[CUSTOMER CITY, STATE ZIP]

Dear [CUSTOMER NAME]:

Last month a laptop computer belonging to Bombay was stolen. Bombay has conducted a thorough investigation of the incident and is notifying you because the laptop contained personal information of 60 Bombay customers, pertaining to individual sales transactions. Though Bombay promptly contacted local police to investigate the theft, we do not expect they will find the computer or the person who stole it.

Two separate files on the stolen computer contained information about you and a purchase you made at Bombay during the latter part of November 2006. One file contained your credit card number, and a separate file contained your name and phone number. Both computer files contained the order number for your purchase, the type of credit card you used, the amount of your purchase, and the date of your purchase. The files did not contain the 3 or 4-digit security code found on your credit card. The specific information about you and your account that was contained in the files is listed below.

Your Name: [CUSTOMER NAME]
Your Phone Number: [PHONE NUMBER]
Your Credit Card Type: [CREDIT CARD TYPE]
Your Credit Card Number (Last 4 digits): [CREDIT CARD NUMBER – LAST 4 DIGITS]

An unauthorized person could link your name to your credit card account number if they combined the information in the two files. However, we believe Bombay's security measures make it unlikely that this will happen. First, your name and credit card number were intentionally separated into two files. This makes it less likely that anyone will link your name to your credit card number if they were able to access the files on this computer. Second, this computer requires a password to be accessed. All Bombay computers, including the stolen computer, are protected by passwords that are at least 8 characters long, and use a combination of upper case letters, lower case letters, and numerals. This password must be entered before a user can access the computer, and is changed periodically for added security. While we believe it is unlikely that anyone will bypass the password, access both files, and combine the information contained in these files, we feel it is important for you to know about this incident so you can take steps to protect your account and personal information.

We value the relationship we have with you, and protecting the security of your personal information is very important to us. We continually evaluate our data security measures to keep your personal information safe. Meanwhile, we encourage you to carefully review all transactions on your monthly credit card statement to be sure that no unauthorized transactions have been made using your credit card. You should also contact your credit card company to discuss other steps that you can take to protect your account. You may also contact any of the national consumer credit agencies listed below to obtain a free copy of your credit report.

Please contact me directly at 817-347-7510 if you have any further questions. We regret any inconvenience this may cause you.

Sincerely,

Steve Sherlock
Vice President Store Operations

Equifax
www.equifax.com
800-685-1111

Experian
www.experian.com
888-397-3742

Trans Union
www.transunion.com
877-322-8228