

SEARS HOLDINGS CORPORATION

Bill Henley
Manager, Unit 5556

Sears Holdings Corporation
3825 Forsyth Road
Winter Park, Florida 32792
Phone: (407) 677-3305
Fax: (407) 677-3254

OCT 18 2006

October 12, 2006

Roy Cooper, Attorney General
NC Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001

Dear Attorney General,

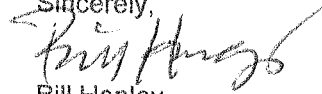
Sears Holdings Corp. ("Sears") is notifying you of a recent incident involving the theft of a Sears'-issued laptop and wireless network card (the "Laptop") from Sears' offices located at 3825 Forsyth Road, Winter Park, Florida, 32792 ("Winter Park") which occurred on Thursday, September 28, 2006. The Laptop was being used by the Winter Park office for a temporary data transfer project. The Laptop contained an Access database file containing certain customer information including names, telephone numbers, addresses, account types, account numbers and expiration dates.

Sears immediately contacted the Orange County, Florida Sheriff's Office on September 28, 2006, to report the incident. The Sheriff's department is continuing to investigate this theft. Sears also promptly began its own internal investigation through its Loss Prevention Department, which is also on-going.

The Laptop was password protected and the file containing the customer data was separately secured by different password information. As well, the database could only be accessed through a Sears' internal connection. Although there is no indication that any of the information from the files has been misused or even disclosed, Sears has sent notification letters to the customers whose confidential information may have been contained in the Laptop.

Sears is committed to protecting the privacy and security of our customer's information. Unfortunately, it is difficult to at all times protect against criminal activity such as the theft of computers. Sears is dedicated to educating it's employees about Sears policies and practices in regard to safeguarding customer information, preventing its unauthorized access, use or disclosure; and, ensuring its proper handling. We are continually seeking to improve our privacy and security practices to prevent future incidents such as this. If you have any questions you may contact me at (407) 677-3305.

Sincerely,


Bill Henley

Attachment

October 6, 2006

[Customer Address]

Dear _____:

The purpose of this letter is to notify you that the theft of a laptop from our offices in Winter Park, Florida may have led to the disclosure of certain confidential information about you. Although there is no indication that any of your confidential information has been misused or even disclosed, we want you to be fully informed so that you can take any steps that you feel are appropriate to protect yourself against identity theft or other criminal activity.

Due to a prior sale of products or services from Sears Home Services organization certain of your credit card data was contained in our computer systems. During a data transfer project at the offices of Sears Holdings Corporation in Winter Park, Florida certain data, including files containing some of your personal information, was temporarily stored on a Sears-issued laptop computer. On September 28, 2006, the laptop was stolen from the office of the Sears employee to whom the laptop had been issued. The office in which the laptop was stored was not readily accessible to members of the general public. That same day we discovered the theft of the laptop and immediately began conducting our own internal investigation. We also immediately contacted the Orange County, Florida Sheriff's Office on September 28, who issued a report that same day.

It is our understanding that the stolen laptop might have contained the following information about you: (1) name; (2) address; (3) phone number; (3) credit card type; (4) credit card number; and (5) credit card expiration date. The laptop and the file were both password-protected. In addition, the files can not be accessed without a Sears' internal network connection.

While we have received no reports of identity theft or fraud associated with the theft of the laptop, we believe it is important for you to be fully informed.

Steps We Recommend You Take

You can take some simple steps to protect yourself against identity theft or other fraudulent misuse of information about you. First and foremost, watch for any unusual activity on your credit card accounts or suspicious items on your bills for the next two years. You may wish to contact your credit card issuers and inform them of what has taken place.

You may also wish to do the following:

- Under federal law, you are entitled to one free copy every twelve months of your credit report from each of the three major credit reporting companies. You may obtain a free copy of your credit report by going on the internet to www.AnnualCreditReport.com or by calling 1-877-FACTACT (1-877-322-8228). If you would rather write, a request form is available on www.AnnualCreditReport.com. You may want to obtain copies of your credit reports to ensure the accuracy of the report information.
- When you receive your credit reports, look the reports over carefully. Look for accounts that you did not open or inquiries from creditors that you did not initiate. Look for personal information that is not accurate. Even if you do not find suspicious activity on your initial credit reports, the California Office of Privacy Protection recommends that you check your credit reports every three months for the next year. Checking your reports periodically can help you spot problems and address them.

- To further protect yourself, you may contact the fraud departments of the three major credit reporting companies. They will discuss your options with you. We have already notified the three major credit reporting companies of this particular incident. You have the right to ask that the three credit reporting companies place "fraud alerts" in your file. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting companies. As soon as that company processes your fraud alert, it will notify the other two credit reporting companies which then must also place fraud alerts in your file.

The three major credit reporting companies are:

Equifax
Report Fraud: 1-800-525-6285
www.equifax.com

Experian
Report Fraud: 1-888-397-3742
www.experian.com

TransUnion
Report Fraud: 1-800-680-7289
www.transunion.com

- To learn more about identify theft and fraud protection, you can go to <http://www.consumer.gov/idtheft>, <http://www.ftc.gov/credit>, <http://www.privacy.ca.gov> or call 1-877-IDTHEFT (1-877-438-4338).

Sears Holdings Corporation is committed to protecting the privacy and security of your personal information. Unfortunately, it is difficult to at all times guarantee against criminal activity such as the theft of computers. We are continually seeking to improve our privacy and security practices to prevent thefts such as this one.

One of our top priorities at Sears is the protection of the personal information of our customers; this is something that we take very seriously. We apologize for any inconvenience or concern this incident has caused.

If we can be of assistance or provide further information regarding this matter, please contact us by mail at the National Inquiry Center, Sears Holdings Corporation, 3825 Forsyth Road, Winter Park, Florida, 32792, by e-mail at credit9539@searshe.com or by phone at (800) 676-5543 Monday through Friday from 8:00 a.m. to 5:00 p.m.

Sincerely,

Bill Henley
Manager, Unit 5556
Sears Holdings Corporation
3825 Forsyth Road
Winter Park, Florida 32792