



Starbucks Coffee Company  
PO Box 34067  
Seattle, WA 98124-1067  
206/318-1575

November 18, 2008

Attorney General G. Steven Rowe  
Office of the Attorney General  
6 State House Station  
Augusta, ME 04333

CONSUMER PROTECTION DIVISION  
RECEIVED

NOV 18 2008

OFFICE OF ATTORNEY GENERAL

Dear Attorney General Rowe:

Pursuant to Maine Revised Statutes, Title 10, §1348, we are writing to notify you that Starbucks Corporation ("Starbucks") recently experienced a data security breach involving 205 Maine residents.

#### **NATURE OF THE SECURITY BREACH**

On October 29, 2008, a laptop computer containing personal information of Starbucks employees, including names and social security numbers, was stolen. The personal information was all electronic, stored on the stolen laptop. The laptop was password protected, and we currently have no indication that the personal information has been misused.

#### **NUMBER OF MAINE RESIDENTS AFFECTED**

The number of Maine residents who may have been affected due to this incident is 205. These residents will all be notified via written letter sent on November 18, 2008, pursuant to Maine Revised Statutes, Title 10, §1348. A copy of that letter is attached for your reference.

#### **STEPS WE HAVE TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT**

The laptop was stolen on approximately October 29, 2008. A police report was filed with the Seattle Police Department shortly thereafter. Starbucks learned of the theft on October 30 and promptly investigated the situation to determine the likelihood that personal information was stored on the stolen computer. When we concluded that the laptop likely did contain personal information of Starbucks employees, we immediately began the process of notifying affected employees of the breach.

In addition, to assist our employees in protecting themselves against potential identity theft, we have contracted with Equifax to offer credit watch services for one year at no cost to the affected employees. The notification letter to employees includes information about how to enroll in the credit monitoring program, as well as the process for placing a fraud alert and other resources relating to identity theft.

As a result of this incident, we are taking the opportunity to once again review our procedures for protecting data and educate our employees about ways to further protect their personal information. We also continue our work to prevent future incidents from occurring and currently are implementing additional encryption solutions where appropriate.



## OTHER NOTIFICATION AND CONTACT INFORMATION

We also are providing notification of this breach to the following consumer reporting agencies: Equifax, Experian, and TransUnion.

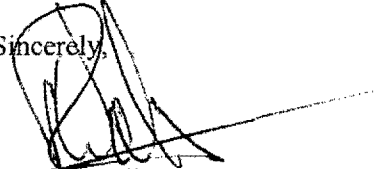
Please do not hesitate to contact me if you have any questions or need further information. My contact information is:

Russell Walker, vp Enterprise Security  
Starbucks Corporation  
2401 Utah Avenue South, Suite 800  
Seattle, WA 98134

(206) 318-7803 (phone)  
(206) 913-6824 (fax)  
[Russell.walker@starbucks.com](mailto:Russell.walker@starbucks.com) (email)

Thank you for your attention to this matter.

Sincerely,



Russell Walker  
vp, Enterprise Security



November 17, 2008

<Partner Name>  
<Address>  
<City, State, Zip Code>

Dear <partner>,

Because Starbucks takes our commitment to safeguarding the personal information and security of our partners very seriously, we are writing to inform you of a recent incident that may have involved a breach of your private information (including name, address and social security number). We are sending this letter to not only notify you about the incident, but also to share information about some safeguarding steps that we recommend you undertake to ensure that your information is fully protected and secure.

Starbucks Enterprise Security learned that a laptop containing partner information was stolen on October 29, 2008. The private information of approximately 97,000 U.S. partners, including yours, was stored on this laptop. A police report was filed with the Seattle Police Department. At present, we have no indication that the private information has been misused.

As a precaution, we ask that you monitor your financial accounts carefully for suspicious activity and take appropriate steps to protect yourself against potential identity theft. To assist you in protecting this effort, Starbucks has partnered with Equifax to offer, at no cost to you, credit watch services for the next year. This service provides you with an early warning of any changes to your credit file. Enclosed you will find a description of the service and enrollment instructions.

In addition, the Federal Trade Commission has released a comprehensive guide that may provide you with valuable information to help protect yourself against and deal with identity theft. It is available for free online at <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html>.

When these incidents occur, we take the opportunity to once again review our procedures for protecting data and educate our partners about ways to further protect their personal information. We also continue our work to prevent future incidents from occurring. In fact, we are currently implementing encryption solutions where appropriate.

Again, while we have no evidence that your personal information has been misused or compromised, we believe it is important that you are fully informed of the potential risks associated with this incident. Starbucks regrets any inconvenience this situation may cause.

If you have any questions, please contact the Starbucks Partner Contact Center at (866) 504-7368.

Sincerely,

Russell Walker  
vp, Enterprise Security  
Starbucks Coffee Company

\*\* Please note that Monday is the busiest day at the PCC, so hold times may be longer than usual. For faster service, you may consider calling during regular PCC hours, Tuesday through Friday.

## The Equifax Credit Watch™ Silver Monitoring System

**Promotion Code: <Mail Merge of Promotion Code>**

Equifax Credit Watch will provide you with an "early warning system" to changes to your credit file and help you to understand the content of your Equifax credit file. Equifax Credit Watch provides you with the following benefits:

- o Comprehensive credit file monitoring of your Equifax credit report with weekly notification of key changes
- o Wireless alerts and customizable alerts available
- o One copy of your Equifax Credit Report™
- o \$2,500 in identity theft insurance with \$250 deductible, at no additional cost to you †
- o 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance and in initiating an investigation of inaccurate information.

### How to Enroll

To sign up online for **online delivery** go to [www.myservices.equifax.com/silver](http://www.myservices.equifax.com/silver)

1. **Consumer Information:** Complete the form with your contact information (name, address and e-mail address) and click "Continue" button. The information is provided in a secured environment.
2. **Identity Verification:** Complete the form with your Social Security Number, date of birth, telephone #s, create a User Name and Password, agree to the Terms of Use and click "Continue" button. The system will ask you up to two security questions to verify your identity.
3. **Payment Information:** During the "check out" process, enter the promotion code, provided at the top of your letter, in the "Enter Promotion Code" box (**include the dash with no spaces**). After entering your code press the "Apply Code" button and then the "Submit Order" button at the bottom of the page. (This code eliminates the need to provide a credit card number for payment.)
4. **Order Confirmation:** Click "View My Product" to access your Equifax Credit Report.

### Directions for placing a Fraud Alert

A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a fraud alert on your credit file, visit: [www.fraudalerts.equifax.com](http://www.fraudalerts.equifax.com) or you may contact our auto fraud line at 1-877-478-7625, and follow the simple prompts. Once the fraud alert has been placed with Equifax, a notification will be sent to the other two credit reporting agencies, Experian and Trans Union, on your behalf.

† Identity Fraud Expense Reimbursement Master Policy underwritten by Travelers Casualty and Surety Company of America and its property casualty affiliates, Hartford, CT 06183. Coverage for all claims or losses depends on actual policy provisions. Availability of coverage can depend on our underwriting qualifications and state regulations. Coverage not available for residents of New York. This product is not intended for minors (under 18 years of age).

## Frequently Asked Questions

### What is a fraud alert and how does it work?

A fraud alert is an advisory placed on a consumer's credit file that alerts potential creditors that the consumer thinks he/she may have been a potential victim of fraud and provides day and evening contact telephone numbers for the consumer to be reached at in the event someone (including the actual consumer) attempts to open an account in the consumer's name. This is a free service.

### Does the one-year credit monitoring subscription start from the enrollment date or from my notification date?

The one-year credit monitoring starts at the time you enroll.

### What happens to the credit monitoring coverage if my employment status changes (or has changed)?

The one-year credit monitoring membership is not contingent on continued employment. Once you enroll, your membership is good for one year. However, you may want to use your personal e-mail address, not your work e-mail address when you enroll.

### If I want to pay to keep the credit-monitoring services for longer than one year, what is the renewal process?

You will automatically be sent a renewal notice 30 days prior to the expiration of the services asking you to renew and provide credit card information for billing purposes. If no response is received, another notice will be sent 10 days prior to the expiration followed by a last chance e-mail. A reminder of the renewal process will also be provided in your member center where you go to access the services. If you do not respond to the renewal requests, the services will be cancelled.

### If I enter my credit card information during the Credit Watch order process, will my credit card be charged?

The credit card will be authenticated for \$1 to validate the card. The \$1 fee will be held by the amount of time pre-determined by your credit card processor, however most processors release the funds within 48 to 72 hours.