

March 24, 2009

Attorney General Kelly A. Ayotte
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Dear Attorney General Ayotte:

I am writing to inform you that Symantec is investigating a potential security incident involving a small number of customers' credit card information.

Symantec is a software company that provides security, storage and systems management solutions. A media outlet in the United Kingdom ("UK") has run a story alleging that, in early March of this year, they purchased three UK residents' credit card numbers from a call center that handles some of our customer transactions. Upon notification, Symantec immediately launched an investigation into the matter, and is working with our call center vendor and law enforcement authorities to determine the facts behind the media claim. The call center agent that we believe is involved had contact with some United States residents.

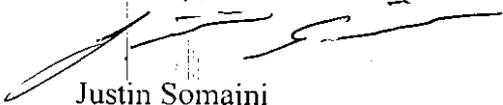
Symantec takes such matters very seriously. We do not believe that a "security breach," as defined in N.H. Rev. Stat. § 359-C:19(I), has occurred for which notice is required; nevertheless, on or about March 25, 2009 we intend to send written notification to one (1) resident of New Hampshire who potentially may be affected by this incident out of an abundance of caution. A copy of the template notice letter that we sent to customers is enclosed.

We have no evidence that the credit card information of any United States resident was actually compromised. As a precaution to help customers detect any possible misuse of personal information, we are providing one year of identity protection services through Debix, Inc. Additionally, we are informing the customers at issue that they should report suspected incidents of identity theft to the U.S. Federal Trade Commission and local law enforcement. We are explaining to them how to place a fraud alert and/or security freeze on their credit file, and are providing the contact information for the national credit reporting agencies.

Protecting personal information is very important to Symantec. We are reviewing our security processes and third party vendor protocols and evaluating additional safeguards to the extent that they are warranted.

If you have any questions, please contact me directly at (650) 527-7448.

Sincerely,



Justin Somaini
VP, Chief Info Security Officer

Debix Activation Code: «**ActivationCode**»

<Name>
<Address Line 1>
<Address Line 2>
<City, STATE>

<Date>

Dear <NAME>,

We recently became aware of a potential security incident involving a small number of customers' credit card information. We have no evidence that your credit card information was compromised, but out of an abundance of caution we are notifying you of this incident.

Symantec is a software company that provides security, storage and systems management solutions. A media outlet in the United Kingdom ("UK") has run a story alleging that in early March of this year, they purchased three UK residents' credit card numbers from a call center that handles some of our customer transactions. Upon notification, Symantec immediately launched an investigation into the matter, and is working with our call center vendor and law enforcement authorities to determine the facts behind the media claim.

We take our obligation to safeguard personal information very seriously. As a precaution to help you detect any possible misuse of your personal information, we are offering you one year of identity protection services through Debix, Inc. at no charge to you. The activation code required to use this service is listed at the top of this page and the instructions for registering for the service are enclosed. We encourage you to regularly review and monitor your account statements and credit reports. The attached Reference Guide provides further details about steps you may wish to take to monitor and protect your credit.

In addition, we have established a dedicated telephone number that you can call if you have any questions. The number – 541-335-7080 – is open Monday through Friday from 8:30 a.m. – 4:30 p.m. PDT.

Symantec is committed to protecting the privacy and security of our customers' information. We are reviewing our security processes and third party vendor protocols and evaluating additional safeguards to the extent that they are warranted. We hope this information is useful to you. We regret any inconvenience or concern caused by this situation.

Sincerely,

Justin Somaini
Vice President & Chief Information Security Officer

Instructions for Registering for Debix, Inc.

Debix Activation Code: «ActivationCode»

User: «FirstName» «LastName»

Symantec has researched available options, and has selected Debix to provide you with Identity Protection Network service at no cost to you for one year. If you are interested in this service, please enroll online via the following URL: www.debix.com/safe. You will need to go to the aforementioned web site and enter the Activation Code at the top of this letter. Once there, click on "Sign up now" and follow the web site's instructions.

Attached is a one page description of the Debix product. You will need access to the Internet, an e-mail address, and a phone to set up your Debix account.

- If you do not have Internet access, you may complete the enclosed mail-in registration form and mail it into Debix.

Once your account is set up, all you will need to be able to use Debix is a telephone, preferably a cell phone. If you do not have a telephone, you will not be able to use Debix. We've chosen Debix since unlike traditional credit monitoring services which only notify you when credit has already been opened in your name, Debix will call you when a creditor is trying to open a new account. Using your phone, you can stop new accounts not initiated by you. Debix is preventative, instead of simply reactive.

Debix will identify new attempts to obtain credit in your name from the date that you set up your account. Debix will not identify any credit accounts that have already been set up in your name.

If you have any difficulties opening new accounts, feel free to contact Debix Customer Support. Their normal hours of operation for phone support are Monday - Friday, 9am - 5pm Central, at 888-DEBIXME (1-888-332-4963).

Reference Guide

We encourage individuals receiving Symantec's letter of [March __, 2009] to take the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually. They provide free annual credit reports only through the website or toll-free number.

When you receive your credit report, review it carefully and look for accounts you don't recognize. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in the information (such as your home address and Social Security number). Errors in this information may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

If you find items you don't understand on your report, call the credit bureaus at the number given on the report. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission. If you detect any unauthorized transactions in your financial account, promptly notify your credit card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission. If you believe your identity has been stolen, the U.S. Federal Trade Commission ("FTC") recommends that you take these additional steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming a victim of identity theft by contacting the FTC:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Place a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	877-478-7625	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, California 92834- 6790	800-680-7289	www.transunion.com

Place a Security Freeze on Your Credit File. You may wish to place a “security freeze” on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze by contacting the credit bureaus at:

Equifax	P.O. Box 105788 Atlanta, Georgia 30348	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, California 92834-6790	www.transunion.com

The credit bureaus may charge a reasonable fee to place a freeze on your account, and may require that you provide proper identification prior to honoring your request.

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at:

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