February 6, 2009

Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Dear Administrators:

In accordance with New Hampshire's data breach notification legislation (N.H. Rev. Stat. Section 359-C:19, - C:20, -C:21), we are writing to inform you that Motorola's Enterprise Mobility Solutions business (also known as Symbol) has recently determined that its Software Technology Center website (http://www.software.symbol.com) has experienced a security vulnerability. This vulnerability may have allowed unauthorized parties to access the personal information of six New Hampshire residents. The personal information of concern includes names, contact information, payment card numbers and payment card expiration dates. The payment card transactions at issue took place during the 2000 – 2005 timeframe (Symbol Technologies, Inc. acquired by Motorola in 2007).

The enclosed set of Questions & Answers provides additional detail concerning this incident. It is important to note that we are working with the third party provider that hosts the website in question in order to investigate and remediate this issue. Moreover, we are taking steps to help prevent a re-occurrence of the security vulnerability in question.

Furthermore, the third party provider has assured us that it will work with Motorola to minimize the risks, if any, associated with this incident. Pursuant to that end, we will soon notify the affected New Hampshire residents of this incident via the enclosed letter.

If you have any questions concerning this matter, please feel free to contact me.

Sincerely,

K. McNeill Taylor, Jr.
Vice President, Law Enterprise Mobility

Enclosures

QUESTIONS AND ANSWERS CONCERNING DATA INCIDENT

INVOLVING HTTP://SOFTWARE.SYMBOL.COM

What exactly occurred?

In mid-January of 2009, an internal Motorola analysis determined that the Symbol Software Technology Center website (**http://software.symbol.com**), which has been in operation since 2000, lacked sufficient security. The Software Technology Center currently allows users to download software updates and to obtain news and information concerning symbol software products. However, from 2000 through 2005, the website also served as an e-commerce store, allowing primarily business users to purchase software products. In particular, certain security flaws in the site at the point of data collection and transmission may have allowed unauthorized third parties to access the site and its database, potentially compromising the personal information of the users of the site.

What personal information was/is involved?

From 2000 – 2005, the website collected name, address, e-mail address, phone number and/or payment card information (i.e., card number, expiration date) of site registrants/customers located in the United States and elsewhere. From 2005 onward, the site only collected contact information of the site's users. With respect to the payment card data involved, it has been determined that, as of January 2009, all but four cards had already expired.

Was the personal information collected via the site encrypted?

Security measures are, by their nature, confidential. However, while registrants' access to the site was controlled via username/password the personal information collected lacked encryption in transit and at rest (i.e., in the database/server).

How will such information incidents be prevented in the future?

Motorola (Symbol) takes such incidents very seriously. Our third-party provider has taken immediate corrective action, including deleting and appropriately disposing of certain data and Motorola (Symbol) is reviewing additional, more stringent security measures for the site. Motorola (Symbol) will continue to review the security measures and processes with them.

How did Motorola/Symbol decide when to notify affected customers/site users?

Once the security vulnerabilities were discovered, some time was required to complete the preliminary investigation and to confirm what information was on the specific databases/servers that were involved. We communicated the information just as soon as we believed it was reliable enough to share.

Is there a risk of identity theft or other harms resulting from a misuse of my personal information?

Currently, we are unaware of any specific risks to particular website users. As mentioned, indications are that all but a few payment cards have expired. Also, given the relative age of the personal information involved, we believe that any risks associated with actual misuse of the data are minimal.

What can I do to protect myself and my personal information from potential misuse?

Be alert. You should check your financial statements (for example, monthly bank or credit card statements) for any unauthorized activity. Report any unauthorized activity to your financial institution and to local enforcement authorities as quickly as possible.

Also, you are entitled under U.S. law to one free credit report annually from each of the three national credit bureaus. To order your free credit report, visit http://www.annualcreditreport.com or call toll-free (877) 322-8228. If you would like more information about Internet safety or identity theft, please visit the U.S. Federal Trade Commission's identity theft web site at http://www.ftc.gov/idtheft.

Note: The following reference guide provides further instructions on preventing oneself from identity theft and related risks.

[Name of Customer]
Address
City, State, Country and Postal Code

Dear **[Name of Customer]**:

We have recently learned that the http://www.software.symbol.com website may have experienced a security vulnerability. We believe that the database related to this website may contain certain personal information about you, including your name, contact information and payment card number(s) ending in **[Last Four Digits of Card Number(s) Affected]**, with an expiration date of **[expiration date related to payment card(s) affected]**. The payment card transactions at issue took place during the 2000 – 2005 timeframe (Symbol Technologies).

We are working with the third party provider that hosts the website to address this issue and are taking steps to help prevent a reoccurrence of the security vulnerability in question. We have taken steps to ensure that the payment card information involved is no longer vulnerable.

We regret that this incident may have affected you. We take our obligation to safeguard personal information very seriously and, therefore, we are alerting you so you can take steps to protect yourself from possible account fraud. We encourage you to remain vigilant and regularly review and monitor your relevant payment card statements. The attached Reference Guide provides details on these and other steps you may wish to consider.

You are entitled under U.S. law to one free credit report annually from each of the three national credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

We hope this information is useful to you. If you have questions regarding this incident, please call toll-free (800) 304-5831 (International and Direct 1-631-738-6419) or send an email to technicalinteractions@motorola.com. If you would like more information about Internet safety or identity theft, please visit the U.S. Federal Trade Commission's identity theft web site at http://www.ftc.gov/idtheft.

Again, we regret any inconvenience this may cause you.

Sincerely,

Reference Guide

We encourage individuals receiving Motorola's letter of February 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 or 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 on your account statement, promptly notify your payment 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

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