170 West Tasman Drive
San Jose, CA 95134-1706
Office: 408.526.4000
Fax: 408.526.4100

April 9, 2012

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

To Whom It May Concern:

In accordance with N.H. Rev. Stat. Ann. § 359-C:20, I am writing to provide you with notification regarding the nature and circumstances of a recent data security incident.

On March 28, 2012, Cisco Systems, Inc. ("Cisco") was informed that certain personal information of a limited number of current and former Cisco employees, as well as some parties associated with recent Cisco acquisitions may have been compromised may have been compromised. A laptop belonging to one of Cisco's service providers, Ernst & Young LLP (EY), was stolen from an EY employee's home on March 26, 2012. The laptop contained personal information including names, addresses, Social Security numbers, and in some cases, stock administration information. At this time, we are not aware of any fraud or other harm to affected individuals as a result of this incident. Cisco is working closely with EY to evaluate data management protocols and help prevent this type of incident from happening again.

Four people who may be affected by this incident reside in New Hampshire. Attached for your reference are sample copies of the notices Cisco and EY are sending to the affected New Hampshire residents Monday, April 9, 2012.

If you have any questions, please do not hesitate to contact me at **rmarenbe@cisco.com** or 408.527.1861

Very truly yours,

Roxane Marenberg

Roxane Marenberg
Sr. Director, Employment Law

LETTER 1
TO: Current Cisco Employees (exposed SSN)
FROM: Cisco
Channel: Email

I am writing to inform you that on March 26th, an employee of Ernst & Young LLP (EY) had a laptop containing your name, Social Security number, home address, and in some cases, stock administration information, stolen during a home break-in. EY provides tax and finance-related services to Cisco, including work related to completed Cisco acquisitions.

Cisco was first informed of this incident on March 28th, and a specialist team of HR, Legal, Privacy, and Information Security representatives was quickly assembled to coordinate the investigation and response. Although we are satisfied that the appropriate laptop security was in place, there remains a small risk of this information being exposed.

We sincerely regret any inconvenience you may encounter as a result of this random crime, and assure you we are working closely with EY to try to make things right. We take the security of this type of data very seriously, and while Cisco's Information Security team has concluded that it is unlikely to be exposed, our primary concern is for your well-being and peace of mind.

You will soon see a follow up message from EY with some important tips for protecting your data, including information about how to access free credit monitoring for one year. We strongly encourage you to read the notice carefully and take advantage of the credit monitoring offer.

EY has also set up a toll-free help line to answer any questions you may have regarding credit monitoring. You may call them at +1 (866) 538-2926 (outside the U.S. or Canada: (201) 872-0955) (Monday-Friday, 9am-6pm EDT until May 31, 2012).

If you have any specific questions for Cisco, please contact the HR Connection on +1 (866) 282-3866 or +1 408 526 5999 from outside the US (Monday-Friday, 9am-8pm EDT). We are also providing these materials on our internal CEC webpage (http://wwwin.cisco.com/HR/hrc/EY2012_Data.shtml).

Please note you will also be receiving a hard copy notification containing this same information.

Again, we regret any inconvenience that you may encounter as a result of this incident. We will continue to work closely with EY to support you.

Regards,

Jim Gemmell
Vice President, Human Resources

LETTER 3
TO: Current Cisco Employees (exposed SSN)
FROM: EY
Channel: Email

As Jim Gemmell's message indicated, an Ernst & Young LLP (EY) employee's laptop was stolen on March 26th. This laptop contained a file that included your name, Social Security number, home address, and in some cases, some stock administration information. Although the appropriate laptop security was installed, there remains a small risk of this information being exposed. Since this occurred, we immediately reported the theft to law enforcement authorities and are working with them on the matter. Additionally, we have worked with Cisco to analyze the data to identify the individuals affected.

EY takes the security and privacy of personal information very seriously, and we sincerely regret any inconvenience you may encounter as a result of this random crime. We have no reason at this time to believe your information has been accessed inappropriately or will be misused, however we want to provide the following information to help you protect yourself:

- We have arranged to provide credit monitoring for one year at no charge to you. To obtain this credit monitoring, you must enroll before October 31, 2012. Once enrolled, you will receive communications detailing any key changes to your credit reports from all three major U.S. credit bureaus. To enroll in this credit monitoring service, please visit the web address below and enter the code provided. You will be instructed on how to initiate your online membership. If you do not have Internet access, please call (866) 252-0121.

  Web site for enrollment: http://partner.consumerinfo.com/ey
  Your Credit Monitoring Code: xxxxxx

- In addition, upon your request, the three major U.S. credit bureaus can place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. There is no charge for this service. However, because it tells creditors to follow certain procedures to protect you, it may delay your ability to obtain credit in some circumstances. You may initiate a fraud alert for all three major bureaus by contacting any one of them at the following numbers or websites:

  Experian (888) 397-3742 www.experian.com
  Equifax (800) 525-6285 www.equifax.com
  TransUnion (800) 680-7289 www.transunion.com

- We encourage you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements and monitoring your free credit reports. You are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

- For additional information on how to further protect yourself against identify theft, you may visit the U.S. Federal Trade Commission's website at www.ftc.gov/idtheft.

- The attached Reference Guide also provides details on these and other steps you may wish to consider.

EY has also set up a toll-free help line to answer any questions you may have regarding credit monitoring. You may call them at +1 (866) 538-2926 (outside the U.S. or Canada: (201) 872-0955) (Monday-Friday, 9am-6pm EDT until May 31, 2012). If you call after hours, please leave a message and we will call you back the next business day.

If you have any specific questions for Cisco, please contact the HR Connection on +1 (866) 282-3866 (Monday-Friday, 9am-8pm EDT). Cisco is also providing these materials on their internal CEC webpage (http://wwwin.cisco.com/HR/hrc/EY2012_Data.shtml).

Again, EY deeply regrets any inconvenience or concern this incident may cause you. We will continue to work closely with Cisco to support you.

Sincerely,

Jeffrey R. Hoops
Partner
Ernst & Young LLP
Chief Privacy Officer

Reference Guide

We encourage individuals to consider 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 ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Please note the credit reporting agencies provide free annual credit reports only through the website, toll-free number or request form listed above.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Be aware that some companies bill under names other than their store or commercial names. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the credit reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the credit reporting agencies 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 reporting agency and relevant creditor(s) by telephone and in writing. 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. You can use the following information to contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft:

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

If you detect any unauthorized transactions in your financial account(s), promptly notify the relevant payment card company or financial institution. If you believe you may be the victim of identity theft, promptly report the incident to your local law enforcement authorities or your state Attorney General, and the FTC. The FTC recommends that identity theft victims take these additional steps:

- Close the accounts that you believe or have confirmed have been tampered with or opened fraudulently. You may use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute unauthorized accounts or account activity.

- File a local police report. Make copies of the police report to submit to creditors or other entities that may require proof of the identity theft crime.

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, a fraud alert informs the merchant that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert by using the contact information provided below. Once you place a fraud alert on your credit file with one credit reporting agency, the alert will be forwarded to the other two agencies. You do not need to place fraud alerts with each of the three credit reporting agencies separately. For more information on fraud alerts, you may contact the credit reporting agencies or the FTC.

Equifax	Equifax Information Services LLC P.O. Box 105069 Atlanta, GA 30348-5069	800-525-6285	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" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the credit reporting agencies without your consent. There may be fees for placing, lifting or removing a security freeze, which generally range from $5-$20 per action. *Unlike a fraud alert, you must place a security freeze on your credit file at each credit reporting agency individually.* Since the instructions for establishing a security freeze differ from state to state, please contact the three national credit reporting agencies or the FTC for more information.

Equifax	P.O. Box 105788 Atlanta, Georgia 30348	877-478-7625	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, California 92834	888-909-8872	www.transunion.com

The credit reporting agencies may require proper identification prior to honoring your request to place a security freeze on your credit file. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Proof of your current residential address (such as a current utility bill)
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may 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 (toll-free in Maryland)
410-576-6300
www.oag.state.md.us

For Massachusetts Residents. The credit reporting agencies may charge you a fee of up to $5 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you provide the credit reporting agencies with a valid police report. You have the right to obtain a police report if you are the victim of identity theft.

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You may contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
877-566-7226 (toll-free in North Carolina)
919-716-6400
www.ncdoj.gov