[INDIVIDUAL NAME]
[ADDRESS (if applicable)]
[DATE]

Dear [INDIVIDUAL NAME]:

WHAT HAPPENED

As part of Cisco's commitment to trust and transparency, we are writing to inform you about an incident potentially involving your personal information.

An independent security researcher discovered that a limited set of job application related information from the Cisco Professional Careers mobile website was accessible. Cisco's investigation found this to be the result of an incorrect security setting following system maintenance. The issue was immediately fixed and passwords to the site have been disabled. Because Cisco takes its responsibility to protect information seriously, and since many people use the same passwords on multiple websites, we wanted to alert you to this incident.

As a precaution, users of Cisco's Professional Careers Website will need to reset their passwords at their next login by clicking "forgot my password".

WHAT INFORMATION WAS INVOVLED

Exposed data included the following data fields: name, address, email, phone number, username and password, answers to security questions, education and professional profile, cover letter and resume text, and voluntary information (if entered) such as gender, race, veteran status, and disability.

Our investigation discovered that the incorrect settings were in place from August 2015 to September 2015, and again from July 2016 to August 2016. We do not believe that the information was accessed by anyone beyond the researcher who found and reported the issue. However, there was an instance of unexplained, anomalous connection to the server during that time, so we are taking precautionary steps.

WHAT WE ARE DOING

We take data protection and transparency very seriously. We continue to investigate the incident and are putting additional protocols in place to help prevent such an incident in the future.

WHAT YOU CAN DO

We recommend that you update/change your login credentials, password and security questions / answers for any other websites that use the same credentials and information as the Cisco Professional Careers mobile website.

Additional Options:

Obtain More Information to Protect Yourself

Visit any of the three US Credit Bureau websites for general information regarding protecting your identity. And the Federal Trade Commission has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

Place a 90-Day Fraud Alert on Your Credit file

An initial 90 day security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Order Your Free Annual Credit Reports

Visit www.annualcreditreport.com or call 877-322-8228.

Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

Manage your personal information
Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

Use Tools from Credit Providers
Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

FOR MORE INFORMATION
Cisco has established an incident response page where you can find the most current information related to this incident: http://www.cisco.com/c/en/us/about/security-center/sto-alerts/2016-security-announce-professional-careers.html

If you have further questions, or would like help from a Cisco representative, please contact Cisco's data incident response team at INSERT EMAIL ALIAS and PHONE NUMBER.

For more information on obtaining free credit reports or identity theft protection:

Experian Experian Security Assistance P.O. Box 72 Allen, TX 75013 Phone: (888) 397-3742 Email: BusinessRecordsVictimAssistance@experian.com	**Equifax** U.S. Consumer Services Equifax Information Services, LLC. Phone: (678)-795-7971 Email: businessrecordsecurity@equifax.com
TransUnion: P.O. Box 6790 Fullerton, CA 92834 Phone: (800) 916-8800 Email: fvad@transunion.com	**Federal Trade Commission** 600 Pennsylvania Avenue, NW Washington, DC 20580 Telephone: (202) 326-2222 (877)-FTC-HELP (382-4357) www.ftc.gov
Your State Attorney General's Office Address Toll free number Website	

Sincerely,
[NAME]
[TITLE]