

February 7, 2008

Director of Consumer Affairs and Business Regulation
Daniel C. Crane
Ten Park Plaza, Suite 5170
Boston, MA 02116

Massachusetts Attorney General
Martha Coakley
McCormack Building
One Ashburton Place
Boston, MA 02108

Mr. Crane and Ms. Coakley:

In accordance with Mass. Gen. Laws ch. 93H (H.B. 4144), we are providing you with written notification regarding the nature and circumstances of a recent event that may constitute a legally-reportable security breach.

We recently became aware of a theft of an unencrypted external storage device. The storage device may have contained the personal information of some current and former salesforce.com employees, including name, Social Security number, and date of birth. Approximately 38 current and former employees affected reside in Massachusetts. At this time, we have no information indicating that the information on the storage device has been misused. Additionally, we have no evidence that any information has been used to commit identity fraud.

Attached for your information is a sample of the notice we plan to send to affected individuals. If you have any questions, please do not hesitate to contact me at (415) 901-8490

Sincerely,



David Schellhase
General Counsel
salesforce.com

Enclosures





February 8, 2008

Dear salesforce.com Colleague:

We recently became aware of a theft of an unencrypted external storage device that may have resulted in the compromise of personal information of some current and former salesforce.com employees. The potentially compromised personal information includes your name, Social Security number, and date of birth. We are working with law enforcement authorities to recover the stolen device. We take our obligation to safeguard your personal information very seriously, and are working to further enhance our data security practices to prevent this type of event from reoccurring.

The personal information was not taken from the salesforce.com application, and no customer data was stored on the stolen device. This theft did not compromise our data centers or our customer security infrastructure in any way.

The storage device was stolen from a vehicle along with several other items. We believe this was a random criminal act, and we have no evidence that the information has been used to commit identity fraud. Nevertheless, to protect yourself, we encourage you to remain vigilant and take the precautions described below to protect against identity fraud and in the attached Identity Fraud Prevention Reference Guide.

To further assist you, we recommend that you register for credit monitoring, which we have arranged to provide you at no charge for twelve months. In addition, you are entitled under U.S. law to one free credit report annually from each of the three national credit bureaus. The attached Identity Fraud Prevention Reference Guide provides information on how you can register for these free services, how to place a fraud alert on your credit file, and recommendations by the U.S. Federal Trade Commission on how to further protect yourself against identity theft.

I hope this information is useful to you. If you would like to speak with us, please email us at response@salesforce.com with your question and the best way to reach you.

We deeply regret any inconvenience that this event may cause you, and we will continue to monitor this situation closely.

Sincerely,

A handwritten signature in black ink, appearing to read "David Schellhase".

David Schellhase
General Counsel

Identity Fraud Prevention Reference Guide

We encourage individuals receiving salesforce.com's letter of February 8, 2008 to take the following five steps:

1. 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. 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. And look in the "personal information" section for information (such as your home address and Social Security number) for any inaccuracies. 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.

2. Register for Credit Monitoring. We have arranged to provide you credit monitoring at no charge for twelve months. Credit monitoring will provide you with an "early warning system" to changes to your credit file and help you understand the content of your credit file. The key features and benefits are as follows:

- Comprehensive credit file monitoring of your Equifax, Experian, and TransUnion credit reports with daily notification of key changes to your credit files from any of the three agencies
- Available wireless and customizable alerts
- One 3-in-1 credit report
- Unlimited access to your Equifax Credit Report
- \$20,000 in identity theft insurance with \$0 deductible (certain limitations and exclusions may apply)
- Live customer service agents available 24-7 to provide personalized identity theft victim assistance and to assist you in understanding the contents of your Equifax credit information and in initiating investigations of inaccurate information

We recommend that you register for this free credit monitoring as soon as possible. To take advantage of this offer, follow this simple Internet-based verification and enrollment process:

- **Visit:** www.myservices.equifax.com/tri
- **Consumer Information:** complete the form with your contact information (name, address and e-mail address) and click the "Continue" button. The information is provided in a secured environment.
- **Identity Verification:** complete the form with your Social Security number, date of birth, telephone numbers, create a User Name and Password, agree to the Terms of Use and click the "Continue" button. The system will ask you up to two security questions to verify your identity.
- **Payment Information:** During the "check out" process, provide the following promotional code: XXXX in the "Enter Promotion Code" box (no spaces, include dash). 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.)
- **Order Confirmation:** - Click "View My Product" to access your 3-in-1 Credit Report

To receive this product by US Mail: Please call toll-free at 1-866-937-8432.

3. 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 there may be fraud on the account. This alerts 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	PO Box 74021 Atlanta, Georgia 30374-0241	1-877-478-7625	www.equifax.com
Experian	PO Box 9532 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division PO Box 6790 Fullerton, California 92834-6790	800-680-7289	www.transunion.com

You will be sent instructions on how to get a copy of your report from each of the credit bureaus. As a possible victim of identity theft, you will not be charged for these copies. Even if you do not initially find any signs of fraud on your reports, we recommend that you review your credit reports carefully every three months for the next year. Just call the numbers above to order your reports and keep the fraud alert in place.

Identity Fraud Prevention Reference Guide

4. Right to Request a Police Report and a Security Freeze on Your Credit Report. You have the right to request a police report and the right to request a security freeze on your credit report. The security freeze will prohibit a credit bureau from releasing any information in your credit report without your express authorization. As such, it could delay or prevent your timely application for new loans, credit, mortgages, insurance, government services or payments, rental housing, employment, investments, licenses, cellular phones, utilities, credit card transactions, or other services, including extensions of credit at the point of sale.

You can request a security freeze by sending a certified, overnight, or regular mail request to the major credit bureaus using the contact information given above. Credit bureaus may charge you a fee of up to \$5 to place a freeze on your account, and may require that you provide proper identification prior to honoring your request. When requesting a security freeze with each of the credit bureaus, you will be required to provide the following information:

For Equifax: your full name, current residential address, date of birth, Social Security number and proof of your current address (such as a current utility bill).

For Experian: your full name, with middle initial and generation (such as Jr., Sr., II, III), Social Security number, date of birth, current address and previous address(es) for the past 2 years. You also will need to provide one copy of a government-issued identification card (such as a driver's license, state or military identification card) and one copy of a utility bill, bank or insurance statement, etc. Make sure that each copy is legible, displays your name and current mailing address and the date of issue. Please note that the statement dates must be recent.

For TransUnion: your name, current residential address, Social Security number, credit card number and expiration date (to pay the \$5 fee). You also will need to provide proof of your current residence (such as a driver's license or state issued identification card).

5. Apply the FTC's Recommendations. 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.consumer.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.
- File your concern with the FTC. The FTC maintains a database of identity theft cases used by law enforcement agencies for their investigations. By filing a concern, it helps the FTC learn more about identity theft and the problems victims are having so FTC representatives can better assist you. The FTC's Identity Theft Hotline toll-free number is 877-IDTHEFT (877-438-4338) or you can visit their website at www.ftc.gov.