

**North Carolina Security Breach Reporting Form
Pursuant to the Identity Theft Protection Act of 2005**

Name of Business Owning or Licensing Information Affected by the Breach: **salesforce.com**
 Address: **The Landmark @ One Market, Suite 300
 San Francisco, CA 94105**
 Telephone: **(415) 901-8490**
 Fax: **(415) 536-4616**
 Email: **dschellhase@salesforce.com**

PLEASE SUBMIT FORM TO:

Consumer Protection Division
 NC Attorney General's Office
 9001 Mail Service Center
 Raleigh, NC 27699-9001
 Telephone: (919) 716-6000
 Toll Free I NC: (877) 566-7226
 FAX: (919) 716-6050

Date Security Breach Reporting Form submitted: **February 7, 2008**

Date the Security Breach was discovered: **January 30, 2008**

Estimated number of affected individuals: **8 in North Carolina, 2,339 overall**

Name of business maintaining or possessing information that was the subject of the Security Breach, if the business that experienced the Security Breach is not the same entity as the business reporting the Security Breach (pursuant to N.C.G.S. §75-65(b)): **n/a**

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: **We recently became aware of the theft of an unencrypted external storage device. The information breached was in electronic format.**

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner: **Not applicable.** If so, please describe the security measures protecting the information: **Not applicable.**

Describe any measures taken to prevent a similar Security Breach from occurring in the future: **We are reviewing and updating our employee data handling policies and procedures. We will supplement our annual online information security training with in-person and online training specifically designed for personal data handlers. We have already implemented technology to identify the transfer of certain types of data via email and the Internet. Soon we will implement similar technology to prevent certain types of data from being transmitted from laptop and desktop computers to external storage devices.**

Date affected NC residents were/will be notified: **February 8, 2008**

If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. §75-65(a) and (c): **n/a**

If the delay was pursuant to a request from law enforcement pursuant to N.C. G.S. 75-65(c), please include the written request or the contemporaneous memorandum.

How NC residents were/will be notified?

(pursuant to N.C.G.S. § 75-65(e))

Please attach a copy of the notice if in written form or a copy of Any scripted notice if in telephonic form.

written notice
 electronic notice (email)
 telephone notice
 substitute notice

Signature: _____

Contact Person, Title: **David Schellhase, General Counsel**

Address: _____

(if different from above)

Telephone: **(415) 901-8490**

Fax: **(415) 536-4616**

Email: **dschellhase@salesforce.com**

Date: **Feb 7, 2008**



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 four 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	800-525-6285	www.equifax.com
Experian	888-397-3742	www.experian.com
TransUnion	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.

4. 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.