

# Deloitte.

December 5, 2007

Office of the Attorney General  
Consumer Protection and Antitrust Bureau  
33 Capitol Street  
Concord, NH 03301  
FAX (603) 223-6202

Deloitte & Touche USA LLP  
Suite 500  
12010 Sunset Hills  
Reston, VA 20190  
USA  
Tel: +1 703 885 6000  
Fax: +1 703 885 6450  
www.deloitte.com

Re: Legal Notice of Information Security Breach Pursuant to N.H. Rev. Stat. Ann. § 359-C:20(i)(b)

To Whom It May Concern:

Deloitte & Touche USA LLP ("D&T USA"), through its subsidiaries, provides audit, consulting, financial advisory, risk management and tax services to selected clients throughout the United States. As you are aware, New Hampshire state law requires notice to the Office of the Attorney General in the event of an information security breach involving the personal information of New Hampshire residents. In accordance with that requirement, we write to inform you of an information security breach concerning personal data of current and former partners, principals and employees of D&T USA and its subsidiaries.

On November 21, 2007, D&T USA's document management vendor, IKON Office Solutions, Inc. ("IKON"), informed D&T USA that a laptop containing a file with information about current and former partners, principals and employees of D&T USA and its subsidiaries had been stolen from an IKON employee's vehicle two days earlier. The file included the names, Social Security numbers, dates of birth and other information relating to those personnel, such as employee hire and termination dates. IKON's employee reported the theft to the Walnut Creek, California police department. The police report number is 07-27609. The laptop was not encrypted, but the laptop was password protected. We have no information indicating the information has been misused.

We estimate that approximately 70 New Hampshire residents were affected by this incident. Pursuant to legal obligations, we are in the process of notifying all affected individuals of the possible information security breach via written letter to each affected individual through first class mail, postage prepaid. Mailing will begin this week. For your convenience, a copy of the notice being sent to the affected individuals is enclosed.

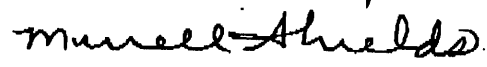
The notices describe (1) the general nature of the incident resulting in the potential information security breach, (2) the type of personal information that was the subject of the possible security breach, (3) the precautionary measures D&T USA is taking to help protect personal information from further unauthorized access, (4) contact information for inquiries regarding the incident, (5) how to enroll in the Triple Advantage<sup>SM</sup> Deluxe credit monitoring service, which D&T USA is making available to affected individuals free of charge for one year; and (6) advice to individuals

Member of  
Deloitte Touche Tohmatsu

that they should also consider placing an initial fraud alert on their credit files and that they review account statements and monitor free credit reports that are available to them.

If you have any questions or need further information regarding this incident, please do not hesitate to contact us.

Sincerely yours,



Murrell Shields  
Chief Privacy Officer, D&T USA

Enclosure

[Insert full name]  
[Insert street address]  
[Insert City address]

[Insert date]

**Re: Important Notice**

Dear [First Name of Individual]:

We are writing to inform you that a laptop computer belonging to one of our outside vendors responsible for scanning our pension fund documents was stolen during Thanksgiving week. The computer contained certain confidential information about you and other current and former partners, principals and employees of Deloitte & Touche USA LLP and its subsidiaries (the "Deloitte U.S. Firms"). Specifically, the computer contained a file that included the names, Social Security numbers, dates of birth, and other information relating to those personnel, such as employee hire and termination dates.

The stolen computer was password protected, but the information on the computer was not encrypted.

Upon learning of the theft, our vendor immediately reported the theft to the local police. So far, the computer has not been recovered. We do not have any evidence that your information has been accessed or misused. However, we recognize the need to provide you with resources so that you can identify any unauthorized use of your data and protect yourself from identity theft.

To enable you to detect any potential misuse of your information, we have arranged for a credit monitoring service to be made available to you, which also includes unlimited access by you to your credit report.

We have contracted with ConsumerInfo.com, Inc., an Experian<sup>®</sup> company, to provide you with one year of credit monitoring, at no cost to you. This credit monitoring service known as Triple Advantage<sup>SM</sup> Deluxe will identify and notify you of key changes in your three national credit reports that may indicate fraudulent activity.

Your 12 month membership includes:

- Monitoring, on a daily basis, all three credit reports with all three major consumer reporting agencies, Experian, Equifax<sup>®</sup> and TransUnion<sup>®</sup>
- Unlimited on-demand access to your Experian credit report and credit score
- Email alerts within 24 hours of key changes indicating possible fraudulent activity
- Monthly "all clear" alerts, if applicable
- Dedicated team of fraud resolution representatives for victims of identity theft
- \$25,000 identity theft insurance with no deductible\*

\*Due to New York state law restrictions, identity theft insurance coverage cannot be offered to residents of New York.

You have until March 1, 2008 to activate this membership, which will then continue for 12 full months from the date of activation. We encourage you to activate your credit monitoring membership as soon as possible. Please visit [insert URL] and enter the activation code provided below. You will be instructed on how to initiate your online membership.

Your Credit Monitoring Activation Code: [insert Activation code]

Whether or not you sign up for the Triple Advantage<sup>SM</sup> Deluxe credit monitoring service, it is always a good practice to regularly review activity on your accounts and to obtain your credit report from one or more of the national credit reporting companies. You should consider contacting the institutions where you hold financial accounts and let them know of the incident so they can notify you of any suspicious behavior or take other steps to protect you. We recommend you remain vigilant for at least the next twenty-four months and that you report any incidents of suspected identity theft to us and to proper law enforcement authorities. **We are also attaching a reference guide based on guidance published by the Federal Trade Commission and other authorities to give you more information about identity theft, how to report it, and how to protect yourself.**

The Deloitte U.S. Firms take the protection of your information very seriously, and we regret any inconvenience or concern that this incident may cause you. We are committed to protecting all confidential information that is entrusted to us. Accordingly, we have suspended all work with the vendor on the pension record scanning project until the vendor can demonstrate that it has implemented appropriate data security protections. In addition, we have an ongoing program to identify vendors who access confidential information regarding our personnel and to confirm that they have implemented appropriate protections.

If you have any additional questions about this incident, please call the Personal Service Network (PSN) at +1 800 DELOITT (+1 800 335 6488) and enter the number 12 (not an option that you will hear in the automated response system) to go directly to people who can answer questions about this incident.

Sincerely,

[Signed by appropriate HR professional]

[Name and title of HR leader]

## IDENTITY THEFT PREVENTION REFERENCE GUIDE

Identity theft, in its simplest form, occurs when someone obtains and misuses your personal information without your permission, and often without your knowledge of the activity.

We urge you to review your credit file monitoring materials carefully for inquiries from companies you did not contact, accounts you did not open, and debts on your accounts that you cannot explain. Verify the accuracy of your Social Security number, address(es), complete name and employer(s). Notify the credit reporting companies if any information is incorrect. You should also monitor any credit cards or consumer accounts you have for suspicious activity. Be sure to report suspected identity theft to the credit reporting companies, to the credit card company and to the proper authorities.

**Free Fraud Alert:** You should also consider placing an initial fraud alert on your credit file. This alert stays on your credit report for 90 days. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. You can do so by contacting one of the three credit reporting companies listed below.

Equifax  
(877) 478-7625  
www.equifax.com  
P.O. Box 740241  
Atlanta, GA 30374-0241

Experian  
(888) 397-3742  
www.experian.com  
P.O. Box 9532  
Allen, TX 75013

TransUnion  
(800) 680-7289  
www.transunion.com  
P.O. Box 6790  
Fullerton, CA 92834-6790

**Free Credit Report:** Even if you elect not to enroll in the Triple Advantage<sup>SM</sup> Deluxe service or place a fraud alert on your file, you are entitled under federal law to a free copy of your credit report from each of the major nationwide credit reporting companies once every twelve months. To order your free report from one or all of the national credit reporting companies, visit [www.annualcreditreport.com](http://www.annualcreditreport.com), call toll-free (877) 322-8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print the form from [www.ftc.gov/freereports](http://www.ftc.gov/freereports). Please do not contact the three nationwide credit reporting companies individually. If you ask, only the last four digits of your Social Security number will appear on your credit reports.

**Credit Freeze:** In some U.S. states, you have the right to put a "credit freeze" on your credit file so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit bureaus at the numbers above to find out more information. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from \$5-20 per action. To place a freeze, you will be required to provide each of the major credit bureaus with your full name, current and former addresses, Social Security number and birth date. If you are not an identity theft victim (for which fees are often waived), you will also be required to provide a check, money order, or credit card payment information.

To learn more about protecting yourself from identity theft, please visit [www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/) or call the Federal Trade Commission hotline: 1-877-IDTHEFT (438-4338).