

**TOWERS
PERRIN**

John Walsh, CISM
Chief Information Security Officer

Centre Square East
1500 Market Street
Philadelphia, PA 19102-4790
215 246-7654
Fax: 215 246-7598

FAX COVER SHEET

Date: <u>January 11, 2007</u>	To:	Fax Number:
No. Pages: <u>7</u> (Including cover sheet)	CSCIC — Security Breach Notification CPB — Security Breach Notification Attorney General — Asst. AG in Charge Bur. of Cons. Frauds	518-474-9090 518-474-2474 212-416-6003

CONFIDENTIALITY NOTICE: The information contained in this facsimile message is privileged and confidential information intended for the use of the addressee listed above. If you are neither the intended recipient nor the employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any disclosure, copying, distribution or the taking of any action in reliance on the contents of this telecopied information is strictly prohibited. If you have received this telecopy in error, please immediately notify us by telephone to arrange for return of the original documents to us.

Message:

Altria Notification —

RESEND —

Notification Letter and D.A. Letters Attached.

PLEASE SUBMIT THIS FORM TO ALL THREE (3) STATE AGENCIES as follows:

Fax this form to the Office of Cyber Security & Critical Infrastructure Coordination (CSCIC) & Consumer Protection Board (CPB):

CSCIC:
Security Breach Notification-
fax: 518-474-9090

CPB:
Security Breach Notification-
fax: 518-474-2474

and also Fax & Mail this form to

Attorney General:
Asst. AG in Charge
Bur. of Cons. Frauds
120 Broadway - 3rd Floor
New York, NY 10271
Fax No: 212-416-6003



**TOWERS
PERRIN**

January 2007

RE: IMPORTANT NOTICE

Dear

Towers Perrin provides benefits and pension consulting services to the Altria family of companies. In some cases, to perform our services, we have access to some of your personal information. On December 1, 2006, we learned that a laptop containing information about you, including your name and Social Security number, had been stolen from Towers Perrin's offices. We deeply regret that this situation occurred and are keenly aware of how important your personal information is to you. We have no reason to believe that your information has been misused. Even so, we want to inform you of the situation and suggest some steps you can take to protect yourself from identity theft now and in the future. We also promptly reported the theft to law enforcement authorities, who subsequently requested that we delay this notification until January 2007 to avoid any possible impediment to their investigation.

We take seriously our commitment to safeguarding confidential information entrusted to us by our clients, like your personal information. All of our laptops and email accounts are password-protected, and some files are password-protected as well. You may rest assured that we are carefully reviewing this incident and are working with Altria to strive to ensure that it does not happen again. Because of this incident, we have accelerated a project we already had underway to encrypt all our laptops by the end of January 2007. In addition, we have engaged an information security consulting firm to review our policies and procedures in the context of this incident to help us assess our areas of vulnerability, target areas for improvement and implement necessary changes.

Precautions You Can Take

Although we have no knowledge of any misuse of your information, **we have arranged for you to enroll, at your option, in the Equifax Credit Watch™ Gold with 3-in-1 credit monitoring product at no cost to you for one year.** The product will provide you with an early warning system for changes to your credit file and help you to understand the content of your credit file at the three credit reporting agencies. To enroll in this product, go to Equifax's website at www.myservices.equifax.com/tri and complete the enrollment process. During the "check out" process, provide the following promotional code: «CODE» in the "Enter Promotion Code" box. Alternately, you may enroll in the U.S. Mail version of the product by completing and sending the enclosed form by mail or via fax to Equifax at the phone number or address shown on the form.

Once you have enrolled, the Equifax Credit Watch™ Gold with 3-in-1 credit monitoring product will provide you with several valuable services including:

- Credit file monitoring of your Equifax, Experian, and TransUnion credit reports;
- Automatic notification of key changes to your credit files from any of the three agencies;
- Free 3-in-1 Credit Report and unlimited Equifax Credit Reports™; and
- 24 by 7 live agent customer service to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance and to help you initiate an investigation of inaccurate information.

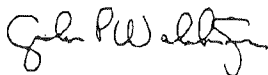
You may also want to consider placing an initial fraud alert on your credit file, which stays on your credit report for 90 days. You can do so by contacting one of the three credit reporting agencies listed below. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. As soon as one credit reporting company confirms your fraud alert, the others are notified to place a similar alert. When you place this alert on your credit report, you will receive information about ordering one free credit report from each of the credit bureaus.

- Equifax: 877-478-7625 www.equifax.com; PO Box 740241, Atlanta GA, 30374-0241
- Experian: 888-397-3742 www.experian.com; PO Box 9532, Allen TX 75013
- TransUnion: 800-680-7289 www.transunion.com; Fraud Victim Assistance Division, PO Box 6790, Fullerton CA 92834-6790

Once you receive your reports, we urge you to review them 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 bureaus if any information is incorrect. You should also be similarly vigilant in monitoring any consumer accounts you have for suspicious activity. Be sure to report suspected identity theft to the credit bureaus, to the company maintaining any compromised account and to the proper authorities. To learn more about how to protect yourself from identity theft, please visit www.consumer.gov/idtheft or call the Federal Trade Commission hotline phone number: 1-877-IDTHEFT (438-4338).

Again, we apologize for any inconvenience or concerns this incident may cause. We are committed to assisting you in protecting yourself. If you have any questions or need additional information, you may contact our information hotline at 800-788-2795.

Sincerely,



John P. Walsh, Jr. CISM
Towers Perrin – Chief Information Security Officer

DEC-29-2006 16:23

MANHATTAN DA OFFICE

DISTRICT ATTORNEY

OF THE

COUNTY OF NEW YORK

ONE HOGAN PLACE
New York, N. Y. 10013
(212) 335-8000



ROBERT M. MORGENTHAU
DISTRICT ATTORNEY

December 29, 2006

Karen M. Allen
Towers Perrin
Managing Counsel - Intellectual Property
1500 Market Street, Centre Square East
Philadelphia, PA 19102

Ms. Allen:

As you are aware, the New York County District Attorney's Office is currently conducting an investigation into the theft of five laptop computers taken from your Manhattan office located at 335 Madison Avenue.

As previously discussed, the loss of the data contained on the computers triggers notification requirements under the laws of many states including New York. However, these statutes specifically allow for a delay of such notification if such delay is requested by law enforcement. Due to a recent arrest and the progression of the investigation into the loss of computers and personal identification information, I ask that you delay the notification process until January 5, 2007. This delay will ensure that the notification does not impede our investigation or progress.

Thank you for assistance and cooperation in this matter.

Respectfully,



Jeremy Saland
Assistant District Attorney