GfK Custom Research
North America

Office of the Attorney General
State of New Hampshire
33 Capitol Street
Concord, New Hampshire 03301

June 29, 2007

Re: Security Breach – Employee Personal Information

Josh Spector
Vice President - Legal Affairs
josh.spector@gkf.com
212-240-5430

To Whom It May Concern:

I am in-house legal counsel for GfK NOP, LLC (d/b/a GfK Custom Research North America) and we are writing to notify your office of a recent security breach involving personal data of certain employees.

On May 29, 2007, a company-owned laptop computer containing password protected files with employee personal information (including name, address and social security number) was stolen. One or more of the affected employees is a resident of the state of New Hampshire.

The attached notification was sent by regular mail to all affected employees on or around June 12, 2007.

Please feel free to contact me if you have any questions or require any further information.

Kind regards,

Josh Spector

GfK Custom Research North America
GfK NOP, LLC
75 Ninth Avenue 5th Floor
New York, NY 10011
USA

Tel 212-240-5300
Fax 212-240-5353
www.gfkamerica.com

GfK Custom Research
North America

First Name Last Name
Address 1
Address 2
City, State Zip

June 4, 2007

Re: Notification of Security Breach

Dear First Name,

On May 29, 2007, an employee who regularly works with our Human Resources Employee Database had her vehicle broken into and Company laptop stolen.

Included on the laptop's hard drive was a password-protected, payroll-related Excel file containing the following information: employee name, state of residence, date of birth, social security number and base rate of pay. We are notifying you of this incident because you are one of the employees whose personal information was included in this file. There is no evidence that any of the personal information contained in the computer has been accessed or utilized. Nonetheless, affected individuals should take steps to protect themselves.

Local law enforcement was notified of the theft of the computer and of the personal information that was contained in some of the computer files.

Here are some steps you can take if you are concerned that a possible breach in your information could result in new accounts being opened in your name.

1. **Notify the credit bureaus and establish a fraud alert** – Call the fraud department of one of the three credit reporting agencies – Experian, Equifax or Trans Union. When you request a fraud alert from one bureau, it will notify the other two for you. Your credit will be flagged with a statement that says you may be a victim of fraud and that creditors should phone you before extending credit. You can place an initial fraud alert for 90 days. You may cancel the fraud alert at any time.
    a. Equifax fraud department: (888) 766-0008 or www.equifax.com

GfK Custom Research
North America
GfK NOP, LLC
75 Ninth Avenue 5th Floor
New York, NY 10011
USA

Tel 212-240-5300
Fax 212-240-5353
www.gfkamerica.com

b. Experian fraud department: (888)397-3742 or www.experian.com/fraud

c. Trans Union fraud department: (800) 680-7289 or www.transunion.com

2. **Order and review your credit report** – Consumers are entitled to one free credit report from each of the three credit reporting agencies listed above during each calendar year. In addition, when you establish an initial alert on your credit report as discussed above, you will be entitled to a free report from each of the reporting agencies. If such a report is not offered to you, request one. Upon receipt of your credit report, closely review the information contained therein, and if there are any accounts you did not open, or credit inquiries for which you cannot account, contact the credit reporting bureau immediately. Also review all of the relevant personal information such as your address and social security number closely to ensure that they have not been altered. If there is any suspicious activity on your credit report, contact your local police department or law enforcement bureau.

GfK will not contact you to verify any of your information, so if an unknown person or entity contacts you seeking any of your information, do not verify or disclose any personal information.

GfK is committed to protecting the security of all personal information it maintains and takes precautions to insure that your information will not be disclosed or otherwise accessed without authorization. We sincerely apologize for any inconvenience this causes and are exploring new ways to safeguard as well as minimize the use of your personal data to prevent possible security breaches in the future.

Sincerely,

Roland F. Fürst
Executive Vice President, General Counsel