



October 6, 2008

Steven G. Rowe, Esq.
Office of the Attorney General
6 State House Station
Augusta, Maine 04333-006

Dear Mr. Rowe:

I am writing on behalf of SGS North America, Inc. and its subsidiaries ("SGS") to inform you of a security breach affecting Maine residents. On July 10, 2008, a thief broke into the car of an SGS employee and stole a briefcase that contained a company-issued laptop computer. The stolen laptop computer contained the names, dates of birth, employee identification numbers, and Social Security numbers of the employees of SGS and its subsidiaries who worked for one of those companies as of June 2008, including 3 Maine residents. The theft has been reported to the Rochelle Park, New Jersey Police Department and is under investigation.

As the result of a breakdown in communication, management employees responsible for responding to this incident did not learn of the theft until August 12, 2008. Since then, SGS has worked diligently to identify affected employees, retain vendors who will be providing assistance to affected employees, and prepare and mail the notice of security breach. SGS mailed its notice to affected individuals on October 6, 2008. A copy of the template letter that was sent to affected Maine residents is attached.

If you have any questions concerning the matters discussed above, please do not hesitate to call me.

Very truly yours,

A handwritten signature in black ink that reads 'Benjamin F. Rodriguez'. The signature is written in a cursive style with a large, stylized 'B' and 'R'.

Benjamin F. Rodriguez
Assistant General Counsel

CONSUMER PROTECTION DIVISION
RECEIVED
OCT 15 2008

OFFICE OF ATTORNEY GENERAL



October __, 2008

[Name of Recipient]
[Street Address]
[City/State/Zip]

Dear [NAME OF RECIPIENT]:

SGS North America and its subsidiaries recognize the importance of safeguarding personnel information. To that end, SGS and its subsidiaries have implemented administrative, technical and physical safeguards for that information. Even the most rigorous safeguards, however, cannot guarantee protection against criminal conduct.

SGS and its subsidiaries recently were victimized by such conduct, and we regret to have to say that this criminal conduct might have a direct impact on you. More specifically, a thief broke into the car of one of our employees and stole a briefcase that contained a company-issued laptop computer. The theft has been reported to the Rochelle Park, New Jersey Police Department and is under investigation.

We have worked diligently to reconstruct the information stored on the stolen laptop. As a result of those efforts, we have been able to determine that the laptop contained the first and last name, date of birth, employee identification number, and Social Security number (SSN) of SGS employees, including yours. We are pleased to report that the stolen laptop was password protected and did not contain any credit or debit card numbers or financial account numbers. In addition, neither the vehicle nor the stolen briefcase would suggest to a passerby the nature of the information stored on the laptop. Consequently, we have no reason to believe that the theft was directed at the information stored on the laptop.

Management employees responsible for responding to this incident first learned of the theft on August 12, 2008. The theft itself occurred on July 10, 2008, but a breakdown in communication delayed reporting to the appropriate executives. We regret that this incident has occurred. We apologize for the delay in our response and for any inconvenience this incident may cause you. We are in the process of reviewing our security procedures in an effort to prevent a recurrence.

At this time, there is no evidence to suggest that there has been any attempt to misuse any information stored on the stolen laptop. Because there remains some risk that your personal information could be misused, SGS North America has contracted with **ID Experts™**, a company that specializes in identity theft protection and fraud resolution, to serve as your principal point of contact and to provide you with comprehensive fraud resolution services, **paid for entirely by SGS North America**. Representatives from ID Experts are available to address any questions or concerns you may have regarding this Incident and protecting your personal information. Just call ID Experts at **1-866-841-7649, Monday through Friday, 6 AM to 6 PM (PT)**. In addition, ID Experts will provide assistance if you suspect that your personal information is being misused. A recovery

advocate will be assigned to your case and will work with you to assess, stop, and reverse any fraudulent activity. If you suspect or discover suspicious activity, you should contact ID Experts immediately at **1-866-841-7649** for assistance.

In addition to the services described above, we have arranged for **one year of free credit monitoring through ConsumerInfo.com, Inc., an Experian® company**. If you choose to enroll in the product membership, known as **TripleAlertSM**, you will benefit from daily monitoring of your credit report at each of the three national credit bureaus, and you will be notified of key changes that may help you to identify possible fraudulent activity. You also will receive monthly "no-hit" notifications if no key changes were detected on your credit reports.

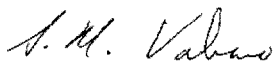
You have ninety (90) days from the date of this letter to activate this membership. We encourage you to activate your credit monitoring membership quickly. Please visit <http://partner.consumerinfo.com/SGS> and enter the activation code provided below. You will be instructed on how to initiate your online membership. If you have any difficulty accessing this product on-line, please call consumerinfo.com at **1-866-252-0121** for assistance.

Your Credit Monitoring Activation Code is **[insert code]**.

For additional information on how to protect yourself against identity theft, please carefully review the **Recommended Best Steps** that are enclosed with this letter.

We have retained ID Experts, a company that specializes in identity theft protection and fraud resolution, so that you can benefit from that company's expertise. Please contact ID Experts directly, at **1-866-841-7649**, if you have any questions concerning this matter. Again, we apologize for any inconvenience that this incident may cause you.

Sincerely,



S.M. Valvano
Senior Vice President
Human Resources

Recommended Steps

By immediately taking the following simple steps, you can help reduce the risk that your personal information will be misused.

1. Contact ID Experts at 1-866-841-7649 to gain additional information about this event and to talk with knowledgeable representatives from ID Experts about appropriate steps to take to protect yourself.

2. Activate the credit monitoring paid for by SGS North America. Credit monitoring is included in the services being offered to you, but you must personally activate it for it to be effective. Note: You must have access to a computer and the Internet to use this service.

The Notification Letter included in this mailing will provide you with instructions and information to activate the credit monitoring portion of the service. If you need assistance, you can contact Experian directly at **1-866-252-0121**. With Experian's credit monitoring, you will receive:

- Unlimited access to your Experian credit report and credit score for one year.
- Notification within 24 hours of critical changes to your credit report. You will quickly find out about changes, including potentially fraudulent activity such as new inquiries, new accounts, late payments, and more.

3. Place Fraud Alerts with the three credit bureaus.

You can place a fraud alert at one of the three major credit bureaus by phone and at Experian also via Experian's website. If you elect to participate in the credit monitoring as discussed above in #2, please wait until **after** you have activated the credit monitoring before placing any fraud alerts. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
(800) 525-6285
P.O. Box 740241
Atlanta, GA 30374-0241

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

TransUnion Fraud Reporting
(800) 680-7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order a credit report from each of the three credit bureaus, free of charge, for your review.

4. Review your credit reports. You can receive free credit reports by placing a fraud alert and through your credit monitoring. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 877-322-8228. You may wish to stagger your requests so that you receive a free report from one of the three credit bureaus every four months.

5. Review your account statements. You should carefully review for suspicious activity the statements that you receive from credit card companies, banks, utilities and other service providers.

6. Contact ID Experts if you see suspicious activity. If you discover any suspicious items in your credit reports or account statements, notify ID Experts immediately by calling 1-866-841-7649.

If you file a theft report with ID Experts, you will be contacted by a member of the Recovery Department who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Experts Recovery Advocate who will work on your behalf to identify, stop, and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items.

8. Additional Information. You can obtain additional information about steps you can take to avoid identity theft from the following:

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.consumer.gov/idtheft
(877) IDTHEFT (438-4338)
TDD: (202) 326-2502