SAIC
From Science to Solutions

**FACSIMILE TRANSMITTAL SHEET**

| TO: | FROM: |
|---|---|
| New Hampshire Attorney General | Amy L. Carlson |
| COMPANY: | DATE: |
| Department of Justice | 1/18/2008 |
| FAX NUMBER: | TOTAL NO. OF PAGES INCLUDING COVER: |
| 603.271.2110 | 4 |
| PHONE NUMBER: | SENDER'S CONTACT NUMBER:: |
| 603.271.3658 | Phone: 206-370-8334 (Holly Towle for Amy Carlson) |
| RE: | YOUR REFERENCE NUMBER: |
| Notice of Data Security Incident | 0324248-00001 |

☐ URGENT ☑ FOR REVIEW ☐ PLEASE COMMENT ☐ PLEASE REPLY ☐ PLEASE RECYCLE

NOTES/COMMENTS:

Greetings:

I write to advise you of a recent incident involving malware which infected a computer owned by Science Applications International ("SAIC"). I am the Chief Privacy Officer for SAIC and my contact information appears at the bottom of this page. I have also included a copy of the form of notice that will be mailed today to two (2) individuals who appear to reside in New Hampshire. Although I am not sure that Section 359-C:20 of the New Hampshire code applies to this situation, which largely involves corporate or entity data, I am providing this notice if only as a courtesy. Thank you for your time and attention.

Amy L. Carlson
Chief Privacy Officer

AMY L. CARLSON
CHIEF PRIVACY OFFICER
1710 SAIC DRIVE, M/S 3-5-9 MCLEAN VA 22102
(703) 676-6397 (O) (703) 448-7732 (F)
AMY.L.CARLSON@SAIC.COM

[date]

[Customer Name/Company/Address]

Dear [name]:

This letter is to notify you of a potential compromise of your company credit card information, including name as it appears on the card, billing and shipping address, phone and fax numbers, credit card number and security code. We collected this information in the process of taking your order in [month] of 2007 for purchase or lease of equipment from our Environmental Equipment and Supply Division.

We recently discovered a single computer used to enter the transaction information you provided by phone was infected with malicious software designed to intercept and log certain keystrokes on the computer. Unfortunately, because the nature of this 'malware' was to intercept keystrokes, it avoided our standard cyber-security precautions (which include encryption of all our hard drives). Although we use industry leading software for virus and spyware detection, the presence of this particular malicious software went undetected until discovered in a regularly scheduled security review of our software inventory.

We have communicated with the Federal Bureau of Investigation to determine the full extent of the malicious software's capabilities. We are also continuing our search for any evidence of information the malicious software may have captured and sent outside of our computer network. Although our network blocks communications to a wide number of IP addresses, it appears that the malicious software may have been able to communicate the information collected to unblocked IP addresses. Consequently, we recommend as a precautionary measure that you consider taking such actions as possible to protect against the potential that someone might have obtained and be in a position to misuse the credit card information provided us in the referenced transaction.

If the cardholder data in question pertains to you individually, as opposed to your company, then please read Exhibit A for information regarding steps we recommend that you consider in order to protect your personal credit. Company accounts do not have all of the same protective rights as do individuals, although some of the steps may be analogous and, therefore, useful.

We apologize for any inconvenience and concern that this situation may cause. Should there be any questions regarding this notice, including questions regarding any potentially compromised information, please call or write Amy Carlson, Chief Privacy Officer for SAIC (phone number: 703-676-6397; mailing address: 1710 SAIC Dr., M/S 3-5-9, McLean, VA 22102).

Sincerely,

SCIENCE APPLICATIONS INTERNATIONAL CORPORATION

Robert F. Shokes
Business Unit General Manager
Engineering & Infrastructure Business Unit

**EXHIBIT A**
**IDENTITY THEFT PREVENTION INFORMATION**

You may take steps to protect yourself against potential misuse of data that has been the subject of a data security incident. The Federal Trade Commission discusses several steps, including obtaining and reviewing your credit report, filing a "fraud alert" and requesting a "credit freeze". The most current and detailed information is available online (see www.ftc.gov/idtheft for general information and http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html for answers to the below questions), but if you are not able to access the linked material, you may also contact the FTC by mail at Federal Trade Commission, CRC-240, Washington, D.C. 20580, or by toll-free number, 1-877-FTC-HELP (382-4357) or 1-877-ID-THEFT (438-4338). You may also contact SAIC's Chief Privacy Officer, Amy Carlson, at 703-676-6397 or 1710 SAIC Drive, M/S 3-5-9, McLean, VA 22102, and she will mail you a copy of the FTC's answers to the following:

1. What are the steps I should take if I'm a victim of identity theft?
2. What is a fraud alert?
3. What is a credit freeze?
4. What is an identity theft report?
5. What do I do if the police only take reports about identity theft over the Internet or telephone?
6. What do I do if the local police won't take a report?
7. How do I prove that I'm an identity theft victim?
8. Should I apply for a new Social Security number?

Fraud Alert: To request a fraud alert, which initially stays active for 90 days and which tells creditors to take reasonable steps to verify your identity before opening new accounts, you will need to contact one of the following credit reporting agencies (see the FTC materials for details). The credit reporting agency is required to notify the other two credit reporting agencies, who will also place a fraud alert on your credit file. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

| | |
|---|---|
| Experian: | 1-888-397-3742; www.experian.com; P.O. Box 9532, Allen, TX 75013 |
| Equifax: | 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241 |
| TransUnion: | 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790. |

Monitor Credit Reports and Accounts: When you receive your credit reports, you should look them over carefully and consider taking the steps recommended by the FTC (see the online materials for details). For example, look for accounts you did not open. Additionally, look for inquiries from creditors that you did not initiate. And finally, look for personal information, such as home address and Social Security number, that you do not recognize. Also, you should monitor your accounts for suspicious activity. If you see anything you do not understand, call the credit reporting agency or provider of your account at the telephone number on the credit report or account statements. If you do find suspicious activity on your credit reports, you may call your local police or sheriff's office and may be able to file a police report of identity theft and obtain a copy of the police report. Potentially, you may need to give copies of the police report to creditors to clear up your records. You may also make a report to the FTC.

Obtain Free Credit Reports: Even if you do not find any signs of fraud on your reports, we recommend that you check your credit report regularly for at least the next one to two years. The Fair Credit Reporting Act requires each of the three credit reporting agencies to provide you with a free credit report, at your request, once every 12 months. You may visit www.annualcreditreport.com, the only Web site authorized by Equifax, Experian and TransUnion for this purpose, to find out more. This website also provides instructions for making a request by phone (1-877-322-8228) or by mailing a request on a form supplied at the site and sending it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA

30348-5281.

Maryland Residents: If you are a resident of Maryland, the contact information for the Maryland Attorney General is Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, 410-528-8662 or toll free at 1-888-743-0023, http://www.oag.state.md.us/. You may obtain information from the Attorney General about avoidance of identity theft.

Massachusetts Residents: Massachusetts law requires provision of the following information, some of which overlaps the federal rights described by the FTC. Under Massachusetts law, you may request that a "security freeze" be placed on your consumer report (a.k.a. credit report) by sending a request to a consumer reporting agency by certified mail, overnight mail or regular stamped mail to an address designated by the consumer reporting agency to receive such requests. If a security freeze is in place, the information from your consumer report is prohibited from being released to a third party without your prior express authorization. According to Massachusetts law, a consumer reporting agency may charge you a reasonable fee, not to exceed $5, if you elect to freeze, lift or remove a freeze to your consumer report. However, if you are a victim of identity theft, a consumer reporting agency must not charge you or your spouse a fee if you have submitted a valid police report related to the identity theft to the consumer reporting agency. You have a right to obtain a copy of your police report.