



Nicole I. Betancourt
Senior Corporate Paralegal
Direct: 703.803.1881
Email: nicole_betancourt@sra.com

VIA FACSIMILE & FEDERAL EXPRESS

January 20, 2009

Maryland Office of the Attorney General
Hugh Williams, Administrator of Identity Theft Programs
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, Maryland 21202

RE: SRA Notice Reporting, Maryland Code Ann., Com. Law §§ 14-3504(h); 14-3504(b)

Dear Mr. Williams:

SRA International, Inc. ("SRA"), pursuant to Maryland Code Ann., Com. Law §§ 14-3504(h); 14-3504(b) is hereby reporting the following official notice below.

The SRA Information Technology Services (ITS) team recently discovered a virus on the SRA network that may have allowed the compromise of data. We immediately launched an investigation into this incident and informed law enforcement and other U.S. governmental authorities. Our investigation into the source of the virus and potential data compromise continues, and SRA's ITS team, supported by SRA cyber security experts, is swiftly implementing mitigation and remediation actions to eradicate the virus.

At this time, we have not determined that any personnel data has been compromised but we believe it is appropriate to notify all employees, former employees and consumers that personal information may have been subject to unauthorized access. The personnel data maintained by the company includes personal information such as name, address, date of birth, health information and Social Security Number, including those of any dependents that are enrolled in SRA benefits programs, as well as personal information stored on a company computer (and which in select cases might include personal data reflected in security position questionnaires) for approximately one thousand three hundred ninety-seven (1,397) residents of the State of Maryland.

As a precautionary measure to help detect any possible misuse of personal information, SRA is offering to its current employees the services of a credit monitoring. Enrollment is not mandatory, and to underscore, we have not determined that any personal information has been compromised.

In addition, SRA has created a dedicated information page on the internal company Web portal. This page will contain tools and resources that address this incident, provide employees with additional details on how to enroll in the credit monitoring service and government Web sites that provide information on how to protect

SRA International, Inc.

4300 Fair Lakes Court • Fairfax, Virginia 22033 • (703) 803-1500 • Fax (703) 803-1509

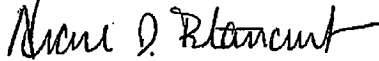
2000 15th Street North • Arlington, Virginia 22201 • (703) 558-4700 • Fax (703) 558-4723

against identity theft. SRA has also set up a special e-mail address to field ongoing questions.

SRA takes the security of personal data very seriously and is committed to minimizing the risks associated with the exposure of personal information. Security is of paramount importance to SRA, and there are numerous safeguards in place to protect information. SRA is implementing additional safeguards intended to prevent a similar incident from occurring in the future.

Should the State of Maryland require anything further, please do not hesitate to contact Mark D. Schultz, Esq, General Counsel, directly at 703.633.2567.

Very truly yours,



Nicole I. Betancourt

cc: Office of the Attorney General, (via Facsimile, Security Breach Notification: 410.576.6566)
Marcy Wilder, Hogan & Hartson (via email: mwilder@hhlaw.com)
Mark D. Schultz, Esq.
Anne M. Donohue, Esq.

Enclosure: Sample copy of distribution notice

FINAL; 01-20-2008; 8:15 p.m.
HARDCOPY
SRA PROPRIETARY



Dear SRA Colleagues:

The Information Technology Services team recently discovered a virus on the SRA network that may have allowed the compromise of data. We immediately launched an investigation into this incident and informed law enforcement and other U.S. governmental authorities. Our investigation into the source of the virus and potential data compromise continues, and SRA's ITS team, supported by SRA cyber security experts, is swiftly implementing mitigation and remediation actions to eradicate the virus.

At this time, we have not determined that any personnel data has been compromised but we believe it is appropriate to notify all employees that personal information may have been subject to unauthorized access. The personnel data maintained by the company includes personal information such as name, address, date of birth, health information and Social Security Number for you and any dependents that are enrolled in SRA benefits programs, as well as personal information stored on a company computer (and which in select cases might include personal data reflected in security position questionnaires). If we subsequently are able to determine that your personal data has been compromised, you will be separately notified.

As a precautionary measure to help detect any possible misuse of your personal information, SRA is offering the services of a credit monitoring company to employees. Enrollment is not mandatory, and to underscore, we have not determined that any personal information has been compromised.

We have created a dedicated [information page](#) on the SRA Portal. You can access this page to find tools and resources that address this incident, obtain additional details on how to enroll in the credit monitoring service and alert you to government Web sites that provide information on how to protect against identity theft. We have also set up a special e-mail address to field ongoing questions: data_security@sra.com, and the [HR specialist](#) assigned to your sector or leverage team is available to answer additional questions.

You should be aware that the information you are receiving today is company proprietary and should not be discussed externally. Refer **media inquiries** to Communication & Public Affairs Vice President Sheila Blackwell (Sheila_Blackwell@sra.com/703.227.8345). We have also begun notifying our customers through our business program managers and contracts personnel. For **customer inquiries**, you should refer questions to Contracts Vice President Mark Connel (Mark_Connel@sra.com/703.322.4969) or CustomerDataSecurity@sra.com.

We apologize for any inconvenience. We want you to know that SRA takes the security of your personal data very seriously and we are committed to minimizing the risks associated with the exposure of personal information. Security is of paramount importance to SRA, and we maintain numerous safeguards to protect your information. We are implementing additional safeguards intended to prevent a similar incident from occurring in the future.

Please take the time to visit the portal page and submit any questions you have to the dedicated employee e-mail address above.

A handwritten signature in black ink, appearing to read "Stan Sloane", is located below the text of the letter.

Stan Sloane
President & CEO

MORE ABOUT SAFEGUARDING PERSONAL INFORMATION

Personnel information – such as names, addresses, dates of birth, personal health information and Social Security numbers as well as personal information stored on a company computer, and which in select cases might include personal data reflected in security position questionnaires – may have been subject to unauthorized access. If your dependents are enrolled in SRA benefits programs, their personal information may also have been subject to unauthorized access. This letter serves as notice to both you, as the employee, plus your spouse and any other dependents you may have enrolled in the SRA health plans. Again, we have not determined that any personal information has been compromised but we do want to share with you the steps you can take to guard against identity fraud.

This and additional information is available on the SRA Portal at <https://info.portal.sra.com/employee/hr/spi/Pages/default.aspx>

Credit Monitoring Services

At your option, we are offering credit monitoring services, at no cost to you, provided by ConsumerInfo.com, Inc., an Experian® company. Please see the dedicated portal page for enrollment instructions if you wish to enroll.

Placing a Fraud Alert

A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report, as well as requests that they contact you prior to establishing any account in your name. Instructions to create an alert can be found [here](#).

Where You Can Go for More Information

If you want to learn more about identity theft, visit the following helpful Web sites:

- The Federal Trade Commission (FTC) runs the U.S. government's identity theft information Web site: <http://www.ftc.gov/idtheft>. You also can contact the FTC by phone at 877.ID.THEFT (877.438.4338).

The Federal Trade Commission

Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
<http://www.ftc.gov/bcp>

If at any time, you find suspicious activity on your credit reports, please file a complaint with the FTC using the online complaint form at <https://www.ftccomplaintassistant.gov/> or call the number listed above. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible by law enforcement agencies for their investigations.

- The Identity Theft Resource Center is a non-profit organization that you can contact online at <http://www.idtheftcenter.org/> or via email to itrc@idtheftcenter.org.

In addition to the FTC, you can also contact the office of your state's attorney general about steps you can take to avoid identity theft.

Experts recommend that you carefully monitor all of your account statements. You may obtain a copy of your credit report each year – free of charge – whether or not you suspect any unauthorized activity on your account. A free copy of your credit report may be obtained by contacting any one of the following national consumer reporting agencies:

• Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

• Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

• TransUnion (FVAD)
P.O. Box 6790
Fullerton, CA 92834-6790

www.equifax.com
800.525.6285

www.experian.com
888.397.3742

www.transunion.com
800.680.7289

FREQUENTLY ASKED QUESTIONS

Q1: What happened?

A1: SRA recently discovered a virus on the SRA network, and through investigation by its cybersecurity experts, determined that it may have allowed the compromise of data.

Q2: What actions have been taken?

A2: SRA has reported the security incident to the appropriate authorities. The IT Services (ITS) team, along with SRA cybersecurity experts are investigating the incident and swiftly implementing mitigation and remediation actions. We have shared our findings with our anti-virus vendor and they have updated their virus definitions to detect the virus files we identified.

Q3: Have other companies been affected by this virus, or just SRA?

A3: Unfortunately, viruses are a common problem. While we have no specific information, we believe that the security issue may affect more than just SRA.

Q4: What kind of personnel data is on SRA servers?

A4: Personnel data maintained by SRA includes personal information such as employee names, addresses, Social Security numbers, dates of birth and health care provider information, as well as those of your spouse or dependents enrolled in our benefits programs. Also potentially subject to access is personal information stored on a company computer, and which in select cases might include personal data reflected in security position questionnaires. At this time, we have not determined that any personnel data has been compromised but we believe it is appropriate to notify all employees that personal information may have been subject to unauthorized access.

Q5: Is this public information?

A5: No. This is proprietary information, but SRA believed it was appropriate to notify employees. Disclosure of this incident may create additional security risks and therefore, should not be discussed publicly. SRA is also notifying customers.

Q6: Was this issue caused by an SRA employee?

A6: At this time, we have no indication that this was caused by an employee. We continue to investigate the incident in collaboration with appropriate authorities.

[More FAQs](#)