



SRA International, Inc.

4300 Fair Lakes Court
Fairfax, VA 22033

703.803.1500 phone
703.803.1509 fax
www.sra.com

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

VIA FACSIMILE & FEDERAL EXPRESS

January 21, 2009

Attorney General Martha Coakley
Office of the Attorney General
One Ashburton Place
Boston, MA 02108

RE: SRA Notice Reporting, Massachusetts, M.G.L.A. c. 93H § 3(a).

Dear Attorney General Coakley:

SRA International, Inc. ("SRA"), pursuant to Massachusetts, M.G.L.A. c. 93H § 3(a), 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 twenty-three (23) residents of the Commonwealth of Massachusetts.

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

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 Commonwealth of Massachusetts 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: Director of Consumer Affairs and Business, (via: U.S. Mail:
Office of Consumer Affairs and Business, Regulation, Ten Park Plaza, Suite 5170, Boston, MA 02116)
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".

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](#)

Choy-Seymour, Shannon

From: Betancourt, Nicole [Nicole_Betancourt@sra.com]
Sent: Tuesday, February 03, 2009 5:29 PM
To: Choy-Seymour, Shannon (AGO)
Subject: Additional notice mailing
Attachments: NB -- Letter to State of MA re additional Notice mailing.pdf

Dear Assistant Attorney General Choy-Seymour,

Thank you very much for taking the time to speak with me yesterday about the additional notice mailing to MA residents. As discussed, attached is a draft notice mailing for your review in advance of our general distribution. Please let me know if you have any comments to the same, as we want to be sure we are compliant with M.G.L.A. c. 93H § 3(a).

Kind regards,
Nicole

Nicole I. Betancourt
Senior Corporate Paralegal
SRA International, Inc.
4350 Fair Lakes Court
Direct: (703) 803-1881 * Fax (703) 803-1509
Mobile: (703) 254-7437
Email: nicole_betancourt@sra.com • www.sra.com



Please consider the environment before printing this e-mail

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

VIA FEDERAL EXPRESS

February 3, 2009

Attorney General Martha Coakley
Office of the Attorney General
One Ashburton Place
Boston, MA 02108

RE: SRA Notice Reporting, Massachusetts, M.G.L.A. c. 93H § 3(a).

Dear Attorney General Coakley:

SRA International, Inc. ("SRA"), pursuant to Massachusetts, M.G.L.A. c. 93H § 3(a), is hereby distributing an additional notice to all Massachusetts residents in the form of the template letter attached. As discussed with Assistant Attorney General Choy-Seymour, and in connection with our correspondence of January 21, 2009, the SRA Information Technology Services (ITS) team recently discovered a virus on the SRA network that may have allowed the compromise of data. In addition to the notification we gave to all residents, which was included our prior mailing, we are sending the enclosed supplement in order to be in compliance with M.G.L.A. c. 93H § 3(a).

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, as well as be in compliance with the Commonwealth's law.

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 Commonwealth of Massachusetts 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: Director of Consumer Affairs and Business, (via: U.S. Mail:
Office of Consumer Affairs and Business, Regulation, Ten Park Plaza, Suite 5170, Boston, MA 02116)
Mark D. Schultz, Esq.
Anne M. Donohue, Esq.

Enclosure: Template copy of additional distribution notice

MA resident
Address
City, MA

Dear _____:

In addition to our recent correspondence to you, the Commonwealth of Massachusetts also provides further protection for residents as outlined below.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. If you provide the credit reporting agency with a valid police report, it cannot charge you to place lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

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

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

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. Include a copy of the police report concerning identity theft;

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique

personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

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.



SRA International, Inc.

4300 Fair Lakes Court
Fairfax, VA 22033

703.803.1500 phone
703.803.1509 fax
www.sra.com

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

VIA FEDERAL EXPRESS

February 4, 2009

Attorney General Martha Coakley
Office of the Attorney General
One Ashburton Place
Boston, MA 02108

RE: SRA Notice Reporting, Massachusetts, M.G.L.A. c. 93H § 3(a).

Dear Attorney General Coakley:

SRA International, Inc. ("SRA"), pursuant to Massachusetts, M.G.L.A. c. 93H § 3(a), is hereby distributing an additional notice to all Massachusetts residents in the form of the template letter attached. As discussed with Assistant Attorney General Choy-Seymour, and in connection with our correspondence of January 21, 2009, the SRA Information Technology Services (ITS) team recently discovered a virus on the SRA network that may have allowed the compromise of data. In addition to the notification we gave to all residents, which was included our prior mailing, we are sending the enclosed supplement in order to be in compliance with M.G.L.A. c. 93H § 3(a).

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, as well as be in compliance with the Commonwealth's law.

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 Commonwealth of Massachusetts 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: Director of Consumer Affairs and Business, (via: U.S. Mail:
Office of Consumer Affairs and Business, Regulation, Ten Park Plaza, Suite 5170, Boston, MA 02116)
Mark D. Schultz, Esq.
Anne M. Donohue, Esq.

Enclosure: Template copy of additional distribution notice



SRA International, Inc.

4300 Fair Lakes Court
Fairfax, VA 22033

703.803.1500 phone
703.803.1509 fax
www.sra.com

MA resident
Address
City, MA

Dear _____:

In addition to our recent correspondence to you, the Commonwealth of Massachusetts also provides further protection for residents as outlined below.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. If you provide the credit reporting agency with a valid police report, it cannot charge you to place lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

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

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

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. Include a copy of the police report concerning identity theft;

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

SRA takes the security of personal data very seriously and is committed to minimizing the risks associated with the exposure of personal information. SRA has no evidence that any of your personal information was compromised, but we believe it is appropriate to notify you in an abundance of caution. 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.

Please refer to the recent correspondence sent in connection with this topic. Should you have any further questions or comments, please contact data_security@sra.com.

Sincerely,

Mark D. Schultz
General Counsel