



CAPITAL COMPUTER ASSOCIATES INC.

FAX TRANSMISSION

To: CPB

Date: 2/20/2006

Company:

Number of Pages: 4
(Including this one)

Fax Number: 474-2474

From: TOM FREDERICK

Message:

SECURITY BREACH NOTIFICATION

Series of horizontal lines for message content.

Reporting Form
For Business, Individual or NY State Entity reporting a
"Breach of the Security of the System"
Pursuant to the Information Security Breach
and Notification Act (General Business Law §889-aa;
State Technology Law §208)

Name of Business, Individual or State Entity: Capital Computer Associates, Inc.
Date of Discovery of Breach: February 16, 2006
Estimated Number of Affected Individuals: 17 (seventeen)
Date of Notification to Affected Individuals: February 17, 2006
Manner of Notification: written notice
 electronic notice (email)
 telephone notice

Are you requesting substitute notice? Yes No (If yes, attach justification)

Content of Notification to Affected Individuals: Describe what happened in general terms and what kind of information was involved. Please attach copy of Notice.

Capital Computer Associates, Inc. provides business management software to Spencerport School District and many other school districts within New York. As a result we have access to personal information of school district employees. We use weekly "Release Notes" to notify our users of changes to the software that they use to process their accounting and human resource data. We use fictitious data for Release Notes, documentation and demonstration purposes. The names and social security numbers of seventeen (17) Spencerport Central School District employees were temporarily posted on the secure area of our company web site and available to be viewed and printed by authorized users as part of our weekly "Release Note" process. The posting occurred on February 14, 2006 at approximately 12:15pm. This error was noticed on February 16, 2006 at 5:45pm and all names and social security numbers were then immediately retracted within 15 minutes. At the time of the retraction it had been posted on the secured area of our web site for approximately 54 hours. The people who were temporarily able to view this information are professional business office staff at our client sites which encompass New York State school districts and BOCES. Since they see screen prints in the Release Notes and documentation similar to the one that was posted all the time, it would be unlikely that they would recognize that this one time the data was real. In addition to removing the sensitive data from the secure area of our web site, we sent out a revised Release Note containing fictitious data for the same date (February 14, 2006) that contained an unrelated additional item added at the end and asked our sites to replace any copies they may have made with the newer version without raising any flags to indicate that they real personnel information. It is our hope, and belief, that this corrective action minimized unauthorized exposure of personnel data.

Name of Business or Individual Contact Person: Tom Frederick
Title: Vice President
Telephone number: (518) 435-0500 ext. 105
Email: tom@cap-comp.com
Dated: _____
Submitted by: Tom Frederick
Title: Vice President
Address: Capital Computer Associates, Inc. 1 Cerone Drive, Albany, NY 12205
Email: tom@cap-comp.com
Telephone: (518) 435-0500 ext. 104 Fax: (518) 435-9464



February 17, 2006

Dear Fred,

It is with much regret and embarrassment that Capital Computer Associates, Inc. must inform you that 17 of your employees had their names and social security numbers temporarily posted on the secure area of our web site and available to be viewed and printed by authorized users of WinCap as part of our weekly release note process.

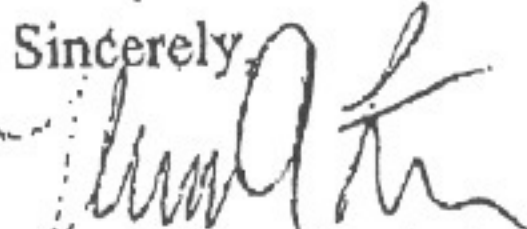
This is especially troublesome to us because we take extra efforts to ensure that an incident like this does not happen. This time there obviously was a breakdown in our procedures and we are dealing with the employees involved while developing even more security procedures to make every effort to ensure that this cannot happen again. Normally we use a fictional version of data for documentation and demonstration purposes. We assure you that we will not use Spencerport data for documentation or demonstration purposes in any form in the future.

On February 14, 2006 at approximately 12:15pm, the employees listed on the attached document were posted on the secure area of our web site with their social security numbers as part of the February 14, 2006 release note. The error was noticed on February 16, 2006 at 5:45pm and was immediately retracted within 15 minutes of when the error was identified. At the time of the retraction it had been posted on the secured area of our web site for approximately 54 hours.

I assume you will be notifying the affected employees pursuant to State Technology Law Section 208 and thereafter notifying the state agencies required to be notified pursuant to the Statute. We will be fully cooperative in any investigation you or they may wish to pursue. Further, Capital Computer Associates, Inc. needs to directly notify such persons under the provisions of General Business Law Section 899-aa. Attached to this letter is the notification which we would like to send to the affected employees and which I think would be best sent with the notification you provide to the employees. Similarly as our obligations to notify state agencies are identical to yours I would appreciate you forwarding the attached notifications to the designated agencies with your notifications.

If we can be of any more assistance in the resolution of this matter, we are here to help.

Sincerely,


Thomas A. Frederick, VP
Capital Computer Associates, Inc.



February 17, 2006

Dear [REDACTED]

Capital Computer Associates, Inc. provides school business office software to [REDACTED] and many other school districts within New York. As a result we have access to personal information of school district employees.

It is with much regret and embarrassment that Capital Computer Associates, Inc. must inform you that your name and social security number was temporarily posted on the secure area of our web site and available to be viewed and printed by authorized users as part of our weekly "Release Note" process. This is especially troublesome to us because we take extra efforts to ensure that an incident like this does not happen. This time there obviously was a breakdown in our procedures and we are dealing with the employees involved while developing even more security procedures to make every effort to ensure that this cannot happen again.

On February 14, 2006 at approximately 12:15pm, your name and social security number was posted on the secure area of our web site as part of the February 14, 2006 Release Note. We use weekly Release Notes to notify our users of changes to the software that they use to process their accounting and human resource data. This error was noticed on February 16, 2006 at 5:45pm and your name and social security number was then immediately retracted within 15 minutes of when the error was identified. At the time of the retraction it had been posted on the secured area of our web site for approximately 54 hours.

We use fictitious data for documentation and demonstration purposes. The people who were temporarily able to view this information are professional business office staff at our client sites which encompass New York State school districts and BOCES. Since they see screen prints for documentation extremely similar to the one that contained your information all the time, it would be unlikely that they would notice that this one time the data was real. In addition, we sent out a revised Release Note containing fictitious data for the same date (February 14, 2006) that contained an unrelated additional item added at the end and asked our sites to replace any copies they may have made with the newer version *without raising any flags to indicate that they had your information*. It is our hope, and belief, that this corrective action minimized unauthorized exposure of your personal data.

In coordination with [REDACTED] we are notifying the State Attorney General, the Consumer Protection Board and the State Office of Cyber Security and Critical Infrastructure Coordination as to the timing, content and distribution of this notice.

We are sincerely sorry for this problem.

Sincerely,

Thomas A. Frederick, VP