



Sachem Central School District at Holbrook

James J. Nolan
SUPERINTENDENT OF SCHOOLS

November 19, 2013

Answers to frequently asked questions from members of the community regarding the theft of student data.

1. When was the Sachem Central School District first informed that student data may have been accessed by an unauthorized person or persons, and what steps did the District take upon learning of that information? There are some claiming that the issue arose this past summer, and some insisting as far back as 2011.

The District became aware that images of a small number of documents relating to certain students were posted on an internet forum in late July 2013. The posting made a general claim that the Sachem database had been "hacked".

The District engaged in an immediate audit of its firewalls and intrusion detection systems. Without revealing the particular nature of what protections that we have in place, or the analysis that was performed, based upon that review, the District has a high degree of confidence that its data systems were not breached from the outside. There were questions as to whether the documents that were posted initially even originated from our District, and whether they originated in digital form.

The District continued to conduct its investigation with confidence that our data systems had not been breached from the outside. We then became aware of allegations that there were additional postings of student information made in August. Upon being made aware of this information, the District immediately contacted the Suffolk County Police Department and filed a police complaint, requesting that this be treated as a criminal matter. We were in contact with both the computer crimes unit and local precinct officers as a part of that reporting process. Upon our investigation and the investigation conducted by the Police at that time, the only records that could be confirmed to have been posted related to information that the Police deemed to be directory information, and / or were maintained in non-digital form. The information that was confirmed to have been posted at that time constituted certain staff names, email addresses and other addresses, none of which contained social security numbers, credit card or driver license information that would trigger additional reporting requirements.

The District again conducted a review of its systems to confirm that it had not suffered a breach from the outside. Again, no such breach was indicated. Based upon that analysis, and the interaction that we had with law enforcement in August, we did not have a belief that an expansive theft of digital data had been effectuated.

The District takes great pride in its students and employees. We believe that the great majority are honest, hardworking individuals who would never conceive of causing harm to a child in any way. But as we have previously stated, access to student records is an important daily internal function of any school district. This is a necessity, but can unfortunately render our data vulnerable to a determined criminal actor willing to misuse access to our systems.

The District also took immediate steps to contact the host site to demand that any post be deleted as quickly as possible. In every instance the host site has been extremely cooperative and has worked to shut down improper posts as soon as we were made aware of them.

2. When and how was Sachem informed of this current breach?

On Friday morning, November 8, 2013, the Superintendent was informed that student information was being posted on a webpage which was linked through a local online forum.

The matter was immediately referred to the Suffolk County Police Department, who took information from us that same morning, November 8, 2013. We have aggressively pursued this complaint with local and federal law enforcement since the moment we became aware of it. We have had extensive contact with both the Suffolk County Police Department and District Attorney's Office, as well as with the Federal Bureau of Investigation. We cannot discuss the specific details of the investigation, but the District remains in constant contact with law enforcement providing any and all assistance that we can provide in furtherance of the investigation.

The District again conducted an immediate audit of its firewalls and intrusion detection systems. Again, without revealing the particular nature of what protections that we have in place or the analysis that was performed, based upon that review the District maintains a high degree of confidence that its data systems were not breached from the outside.

3. Does Sachem know which files or what kind of information has been compromised?

The District can only definitively comment on those documents which have been revealed to date. We are doing our best to keep the public reasonably informed without creating the potential for misinformation, or discussing matters that could compromise the investigation into this matter. Notices compliant with the New York State Technology Law and General Business Law are being generated to individuals whom we reasonably believe were affected by this criminal act. We have been in contact with the Office of the New York State Attorney General in this regard as well.

4. Is Sachem required to now offer credit protection/identity theft protection to the people whose files have been compromised? If yes, when will that begin? If no, will they offer it anyway?

Not at this time. The law requires that individuals whom the District reasonably believes have been affected be notified so that they may take appropriate action, and those notices have been generated and should be received by the affected individuals shortly if they have not received them already.

5. If a person has downloaded the information and it does not pertain solely to themselves or their child, can they get in trouble?

We believe so, yes. The District has devoted every available resource to cooperate with and to assist Law Enforcement. It is our sincere hope that the perpetrator of these acts is apprehended and prosecuted.

6. If any information regarding my child has been posted online, when will we receive the notification?

We are in the process of making legal notification to anyone that we reasonably believe was affected. We have also posted information on our website about the general nature of what we know at this point.

7. What information does the district know has been posted in the November incident?

A list of 15,000 names with student ID numbers and school lunch designation. No other information was attached to that list. The posted list appears to be a list of students from the early 2000's.

Another list of 12,000 names with student ID numbers, with no other information attached. All but approximately 900 of this list were also contained in the previously mentioned list of 15,000.

Student records relating to approximately 360 students who graduated from Sachem High School East in 2008.

A report relating to approximately 130 students who attended Sachem High School North who were receiving instructional services in an alternative setting in the 2010-2011 school year.

Obviously the improper access of any records whatsoever gives us concern about the potential scope of what could have been compromised, but that is the list of what the District is aware was posted.

To be safe, the District has sent notices to the last known addresses of all of these individuals, and to an additional group of approximately 360 individuals whose records were stored in the same folder of the records we believe to have been compromised in some fashion.