Data Breach Accessed 160,000 Student’s Information

Kevin Miller

[Millke03@metrostate.edu](mailto:Millke03@metrostate.edu)

Approximately 160,000 current and former students at Metropolitan State University had some of their personal information accessed in a December 2014 data breach. About 25,000 of those students currently attend Metro. No financial information was compromised. However, demographic information, personal information, academic information (including Star and Tech IDs), and the last four digits of Social Security numbers were accessed. Students whose data was accessed were contacted, either by e-mail or US mail. Those students can also receive support through an identity theft protection firm called Kroll. About 900 faculty members also had their data accessed in December.

Have Any Identities Been Stolen?

The University does not know of anyone whose identity has been stolen.

“At this point, we haven’t heard from any faculty, or staff, or students who have had a data breach who have had any identity theft,” said Anne Sonnee interim Vice President of Advancement and Communications at Metro.

Investigation Finished

Three different agencies worked together to conduct an investigation into the data breach, according to Sonnee. One of those was MN.IT, Minnesota’s governmental information technology service. They collaborated with Minnesota State Colleges and Universities (MnSCU) information technology department and Metro’s information technology department.

Their study was concluded this April, after announcing that student data had been accessed.

“It’s kind of been concluded in phases,” said Sonnee. “That first phase was concluded in February, which is when they determined that there was the 900 faculty members who had their Social Security numbers breached. They kept digging to decide ‘well, was there anything else?’ That’s when they started looking more into the student data and learned there had been some additional data [accessed]. That was concluded in April.”

The US Secret Service is working on its own investigation into the hacking. Sonnee said the administration is waiting to hear the results.

Who Was the Hacker?

Sonnee said the actual identity of the hacker may not be who the individual claimed to be online. That said, he or she is allegedly a 16 year old Australian.

This individual bragged about hacking Metro and several other schools on a forum. It was seen by an outside vendor who alerted MnSCU. The hacker was allegedly inspired to hack Metro after watching the movie “22 Jump Street,” as the main characters attend a fictional university called “Metro City State.” The suspect is also allegedly in custody of the Australian government.

Identity Theft Protection Services

A vendor named Kroll will provide identity theft protection services for affected students and faculty. Sonnee said since faculty had their full Social Security numbers exposed, they are eligible for a year of Kroll’s identity theft protection service package and their credit monitoring service.

Metro purchased a different package for students. Those with the last four digits of their Social Security number exposed have Kroll’s identity theft protection service package. Kroll will refer students to a free credit monitoring service that is not affiliated with their own work.

Sonnee said students who had their data accessed should call Kroll to begin the protection process. “They have expert consultants who will walk you through what you should be watching out for, or concerned for.”

Hoax Phone Calls

Some Metro students have received phone calls from people claiming to be with the Minnesota Department of Education, asking the students to confirm their personal information. Sonnee, said around a dozen others have reported hoax phone calls, although they were not from agents claiming to be with MN Dept. of Ed. Sonnee said the administration does not know if these calls are in connection with the data accessed in December.

“I’ve probably had a dozen phone calls since we sent that e-mail out asking people to notify me if they had anything that seems suspicious,” said Sonnee. “Only two or three specifically said it was the Department of Education that called them. Otherwise, they were random ‘I have an uncle in Nigeria that wants to send you money’ kind of calls, and I don’t that we can connect that.”

“If you receive such a call, you can assume it is a scam and should not provide any information,” said an April 27 e-mail to students. If you do receive such a phone call, you should contact Sonne at [anne.sonnee@metrostate.edu](mailto:anne.sonnee@metrostate.edu) or 651-793-1805.

MnSCU Security Changes?

MnSCU’s head office stores student information in its Integrated Statewide Record System (ISRS). Charting the Future, MnSCU’s program driving its upcoming economic and educational decisions, wants to replace ISRS. It said ISRS uses “aging and outdated software tools.” Moreover, Charting the Future’s documentation said ISRS “hampers MnSCU’s ability to keep up with current education and software trends.” This system is separate from Metro’s server.

Sonnee said MnSCU was concerned about the possibility of the breach reaching ISRS, so MnSCU took preventative measures to increase security.

Ramone Padilla, Jr. is acting Chief Information Security Officer at MnSCU. “We take our responsibility to protect student and employee data very seriously and are working hard to ensure the right safeguards are in place,” he said. “We made immediate adjustments to our security posture and will make further adjustments in the future based on this and other threat data we get from our security partners.”