Connecticut Post

Tuesday, April 5, 2011

EMAIL, CREDIT CARDS AT RISK

Data breach hits state

By Rob Varnon
Staff Writer

College-bound students, credit card users and employers looking to hire professionals are among the Connecticut residents whose email addresses may have been accessed by hackers who broke through the firewall of a Dallas-based advertising and email management firm.

The security breach at Epsilon occurred late last week and allowed for unauthorized access to the email distribution lists belonging to JP Morgan Chase, Citigroup, Robert Half International, the College Board, Walgreens, TiVo and other companies. Epsilon said in a statement on Monday that about 2 percent of company's clients were affected.

Many of those affected were people who provided emails when applying for a credit card or discount club. In the case of the College Board, which administers the SAT and other college preparatory tests, the addresses were provided by students.

"The information that was obtained was limited to email addresses and/or customer names only," Epsilon said in its statement. "A rigorous assessment determined that no other personal identifiable information associated with those names was at risk. A full investigation is currently under way."

The Connecticut Attorney General and departments of Consumer Protection and Banking said staff are monitoring the situation, and so far few, if any, complaints had reached them on Monday. All three agencies were looking into the matter.

Attorney General George Jepsen sent a letter to the company Monday asking for more information about the breach.

"The situation also raises questions about the effectiveness of Epsilon's measures to protect the confidentiality and security of private information that it receives from its clients — and, by extension, their customers. I am particularly concerned that breaches of this sort do not reoccur and that affected individuals are provided sufficient protections to safeguard their information from further disclosures," Jepsen said.

The State Department of Consumer Protection on Friday had issued a report that showed Connecticut residents lost $3.3 million in scams last year.

That's the biggest problem with this breach, according to Tarek Sobh, the dean of the University of Bridgeport's School of Engineering. He said it provides a direct line to a live email for a thief who will be able to provide what looks like a legitimate email and then ask for private information.

"Inevitably, some people will think its legitimate and all of a sudden, their own systems are completely open," said Sobh, who specializes in computer engineering.

The type of email marketing that companies like Epsilon carry out requires expensive hardware and software that many corporations would rather outsource, according to Sobh.

Plus, there are other ramifications.

"We will get lots of spam," he said.

Whoever got the lists will be selling them around the globe — probably on legitimate looking sites — for reduced prices. Sobh said lists of legitimate customers, especially credit card users, are valuable and costly.

For Epsilon and its customers, "This is a disaster," he said. Someone could be held liable for the slip-up, he said, since most of the emails were given to companies like Citigroup with the understanding that they would not be sold or shared with a third party.

Epsilon is also in a competitive field, Sobh said, which is evident from the fact that many local banks and businesses said they were not affected by the breach.

While affected businesses were notifying customers, many other banks and organizations reported no problems.

General Electric Co.'s GE Money, which provides branded credit cards to retailers, said it wasn't affected. Nor were People's United or Webster Bank.

The state's largest grocer, Stop & Shop doesn't use Epsilon either.

"We do a combination of internal management as well as outside vendors," said Suzi Robinson, a Stop & Shop spokeswoman. "Ensuring customer information is protected is always a priority. We follow all regulations and are very careful with customer data."

For now, people are being asked to be careful.

Hackers may have access to data