Targeted nature of email breach worries experts

April 4 2011, By JORDAN ROBERTSON and PETER SVENSSON , AP Technology Writers

Think twice next time you get an email from Chase or Citi asking you to log in to your credit card account. The bank may not have sent it.

A security breach that exposed the email addresses of potentially millions of customers of major U.S. banks, hotels and stores is more likely than traditional scams to ultimately trick people into revealing personal information.

Security experts said Monday they were alarmed that the breach involved targeted information - tying individuals to businesses they patronize - and could make customers more likely to reveal passwords, Social Security numbers and other sensitive data.

The company that was in charge of the email addresses, a Dallas marketing firm called Epsilon, handles online marketing for some of the biggest names in business. Those companies have flooded customers in recent days with warnings to be on guard.

Epsilon said that while hackers had stolen customer email addresses, a rigorous assessment determined that no other personal information was compromised. By itself, without passwords and other sensitive data, email addresses are of little use to criminals. But they can be used to craft dangerous online attacks.

Citi credit card customers, for example, are more likely to respond to an

email claiming to be from Citigroup than from a random bank. The email might direct the customer to a site that looks like the bank's site, capture login information and use it to access the real account.

David Jevans, chairman and founder of the nonprofit Anti-Phishing Working Group, said criminals have been moving away from indiscriminate email scams, known as "phishing," toward more intelligent attacks known as "spear phishing," which rely on more intimate knowledge of victims.

"This data breach is going to facilitate that in a big way," said Jevans, also CEO of security company IronKey Inc. "Now they know which institution people bank with, they know their name and they have their email address."

The information could also help criminals send highly personalized emails to victims. Doing so makes the email more likely to get past a spam filter.

Epsilon, a unit of Alliance Data Systems Corp., sends more than 40 billion emails a year and has more than 2,500 business clients. Stock in the parent company fell $1.73, or 2 percent, to close Monday at $84.20.

Meanwhile, more than a dozen companies contacted customers to instruct them never to reveal personal information in response to an email.

Financial institutions affected include Barclays Bank, Capital One Financial Corp., Citigroup, JPMorgan Chase and U.S. Bancorp. The parent companies of Best Buy, Ethan Allen furniture stores, the Kroger grocery chain, the Home Shopping Network and Walgreens drugstores issued similar warnings, as did the Hilton and Marriott hotel chains. The College Board, the not-for-profit organization that runs the SATs, also

warned that a hacker may have obtained student email addresses.

Many of the companies contacted by The Associated Press declined comment or referred reporters to statements acknowledging the breach. Epsilon also declined further comment. Some of the companies said Epsilon has referred the breach to unspecified authorities.

For victims of this type of security breach, there is little to do but be vigilant. Changing passwords doesn't help.

Jill Kocher of Crystal Lake, Ill., said she got at least five emailed warnings, including from U.S. Bank, Best Buy and clothier New York & Co. Because she works for Groupon, an Internet coupon company, she said she feels savvy enough to avoid any phishing come-ons. But she's concerned for those who aren't.

"U.S. Bank sends you an email and it looks legit and you cough up the information, and now you're in big trouble. It sure does sound like a big increase in fraud just waiting to happen," Kocher said.

The attack offers a window into a business that serves a vital role in the Internet age for companies looking for effective ways to find customers, sell to them, and figure out what they might want to buy in the future.

Epsilon is a big moneymaker for Alliance Data Systems. Epsilon turned $65 million in operating profit last year, and its $613 million in revenue was 22 percent of Alliance Data Systems' total.

Companies like Epsilon send emails to customers on behalf of companies, using vast stores of data and millions of addresses. Companies are eager to give up information about their customers - if the third parties such as Epsilon can do a better job at enticing them to spend.

So for example, an email that a retailer blasts to customers about an upcoming sale on big-screen TVs might not actually come from the company at all. A company such as Epsilon might be the one that analyzed the spending of that store's customers and decided which ones would be most likely to buy a big-screen TV.

Dave Frankland, an analyst with Forrester Research who studies Epsilon and other businesses that specialize in "customer intelligence," said large companies often outsource their email marketing to avoid being having their messages zapped by email service providers' spam filters. Companies such as Epsilon work with the email providers to ensure that their customers' messages aren't blocked as spam. He said that is a job that requires daily attention.

Frankland said the industry's reputation will take a hit because the breach exposed how much the relationships between companies such as Epsilon and their customers depend on trust.

"At first glance, I shrug my shoulders and go, `Oh my goodness - a spammer knows my name,'" he said. "I get enough spam; that isn't new. But the bigger concern is when someone gets an email from one of these blue chip companies and it looks genuine. That's when I get very concerned."

But he added: "The industry should be looking at this as a let-off. This could have been a heck of a lot worse. It's not just Epsilon - it's an industry issue, and this could have been any of them."

Breaches involving millions of customers have happened before. In one of the largest, more than 45 million credit and debit cards were exposed to possible fraud because of hackers broke into the computer system of TJX Cos., the parent company of retailers T.J. Maxx and Marshall's, starting in 2005.

And last month, RSA, the security division of data storage company EMC, acknowledged that its computer network was hacked. The implications are serious because RSA's technology underpins the security of some of the world's most closely guarded data. RSA makes small security devices that supply constantly changing numbers that are used as secondary passwords for accessing corporate networks and email.

If the attacker managed to steal the codes that determine which numbers appear on the tokens, that information could be used to perform mass infiltrations - if the attacker already has other information about the targets. That information can be gleaned from the type of "spear phishing," or targeted phishing, emails that the Epsilon breach can enable.

"I'm a little concerned that there's a big pattern going on here of very major breaches, where if you combine that information together, you could launch some pretty major attacks that would be very successful," Jevans said.