The New York Times

BUSINESS DAY

After Breach, Companies Warn of E-Mail Fraud

By MIGUEL HELFT APRIL 4, 2011

SAN FRANCISCO — Security experts said Monday that millions of people were at increased risk of e-mail swindles after a giant security breach at an online marketing firm.

The breach exposed the e-mail addresses of customers of some of the nation's largest companies, including JPMorgan Chase, Citibank, Target and Walgreens. In some cases customer names were also stolen.

While the number of people affected is unknown, security experts say that based on the businesses involved, the breach may be among the largest ever. And it could lead to a surge in phishing attacks — e-mails that purport to be from a legitimate business but are intended to steal information like account numbers or passwords.

"It is clearly a massive hemorrhage," said Michael Kleeman, a network security expert at the University of California, San Diego.

The marketing firm that suffered the breach, Epsilon, which handles e-mail marketing lists for hundreds of clients, disclosed the problem in a brief statement on Friday. But its sheer scale became clear over the weekend and on Monday, as banks, retailers and others began alerting their customers to be on the lookout for fraudulent e-mails.

While e-mail addresses may not seem particularly vulnerable, experts say that if criminals can associate addresses with names and a business like a bank, they can devise highly customized attacks to trick people into disclosing more confidential information, a technique known as "spear phishing."

"Any time you have an organization that loses the contact information of customers for some of the biggest banks in the world, that's a big deal," said Brian Krebs, editor of Krebs on Security, a Web site that specializes in online security and crime. "You've just given the bad guys a road map between the banks and their customers."

In traditional phishing attacks, criminals e-mail millions of people with a message that appears to be from a bank or other real business, hoping that some of the recipients will be customers of that business and will follow instructions to, for example, "update your account information."

A spear-phishing e-mail is far more dangerous because it can include a person's name and is sent only to people who are known to be customers of a certain business, greatly increasing the likelihood that the targets will be duped.

Phishing has remained a major challenge, especially for banks and other financial institutions, which want to encourage customers to do business with them online.

The Anti-Phishing Working Group, an organization that tries to prevent Internet crime, received reports of more than 33,000 phishing attacks worldwide last June, the most recent month for which data is available. Roughly 70 percent of the attacks were in the financial services and online payment industries.

With the information stolen from Epsilon, thieves could send customers of a particular bank an e-mail that appeared to be from the bank, complete with their names, said Mark Seiden, an information security consultant in Silicon Valley. If the criminals cross-check a name with the property records of mortgage holders, they could even include the customer's address in the e-mail, he said.

"Something that is that customized and has the right graphical elements, people will fall for it," Mr. Seiden said.

The companies that alerted customers or acknowledged being affected also include Barclays Bank, U.S. Bancorp, Walt Disney, Marriott, Ritz-Carlton, Best Buy, L. L. Bean, Home Shopping Network, TiVo and the College Board.

In e-mails to their customers, the companies asked them to be cautious but also sought to reassure them that the hackers had obtained only e-mail addresses and in some cases names, not passwords, account numbers, credit card information or other more confidential data.

"Your account and any other personally identifiable information were not at risk," the clothing retailer New York & Company told its customers in an e-mail. "Please note, it is possible you may receive spam e-mail messages as a result. We want to urge you to be cautious when opening links or attachments from unknown third parties. We also want to remind you that we will never ask you for your personal information in an e-mail."

Ron Baldwin, a technology consultant in Laguna Niguel, Calif., said that over the weekend he received an e-mail alerting him to the security breach from U.S. Bank, where he is a customer. He said he was particularly upset that the bank, a unit of U.S. Bancorp, would entrust his information to another company.

"They shared my information with a third party unbeknownst to me," Mr. Baldwin said. "I don't know Epsilon from some guy walking down the street." Mr. Baldwin said that when he contacted the bank, he was told that he had given permission to share information with suppliers.

Jessica Simon, a spokeswoman for Epsilon, which is based in Irving, Tex., said in an interview: "We are currently working with authorities and are conducting a full investigation. We are limited in what we can share."

Epsilon is a unit of Alliance Data and has some 2,500 clients, though not all of them use its e-mail marketing services. The company said that about 2 percent of its clients were affected. It declined to say how the hack had occurred or why the e-mail addresses had not been encrypted.

"Epsilon has some explaining to do about the numbers, how it was penetrated and what they have done to protect the information they have," said Mr. Kleeman, the security expert.

Mary Landesman, a senior security researcher at Cisco Systems, said that because e-mail addresses were not considered of great value in the criminal underground, she suspected the attack on Epsilon began as something random. Hackers often scan the Internet looking for machines that have a certain vulnerability or misconfiguration and then, once they hit upon something, look further to see if the victim interests them. Ms. Landesman speculated that the attackers had found themselves on Epsilon's system, realized what they had and then worked to acquire their customer lists.

The breach points out the significant risks for companies that outsource even seemingly low-risk activities like e-mail marketing, said Avivah Litan, an analyst focused on online fraud at the research firm Gartner. It also highlights the lack of regulation on security when it comes to consumer data that is not directly tied to financial accounts, which are subject to industry standards, Ms. Litan said.

Correction: April 4, 2011

An earlier version of this article misspelled part of the name of a city in California where Ron Baldwin is a technology consultant. It is Laguna Niguel, not Laguna Nighel.

Correction: April 7, 2011

An article on Tuesday about a major security breach at the online marketing firm Epsilon misstated the information that was exposed from three of Epsilon's clients: JPMorgan Chase, Target and Walgreen. Only e-mail addresses were exposed, those companies said — not customer names. (Many Epsilon clients reported the exposure of both e-mail addresses and names.) A picture caption with the article repeated the error about one client, JPMorgan Chase.

Riva Richmond and Stephanie Clifford contributed reporting from New York.

A version of this article appears in print on April 5, 2011, on Page B1 of the New York edition with the headline: Firms Warn of E-Mail Fraud After a Breach.
