GEORGE JEPSEN
ATTORNEY GENERAL

STATE OF CONNECTICUT

OFFICE OF THE ATTORNEY GENERAL

DEPARTMENT OF CONSUMER PROTECTION

WILLIAM M. RUBENSTEIN
COMMISSIONER

CONSUMERS ADVISED TO SCREEN E-MAIL CAREFULLY FOLLOWING WIDESPREAD DATA BREACH OF EPSILON

For immediate release MONDAY APRIL 4, 2011

HARTFORD – Attorney General George Jepsen and Consumer Protection Commissioner William Rubenstein are advising Connecticut consumers to screen e-mail carefully and not to respond to requests for personal or account information, including login names or passwords.

The advisory was issued after Epsilon Data Management LLC, an Irving, Texas company that describes itself as the "world's largest permission-based e-mail marketing provider," informed its clients that Epsilon's e-mail system had been breached by an "unauthorized entry." A statement on Epsilon's website said "the information that was obtained was limited to e-mail addresses and/or customer names only. A rigorous assessment determined that no other personal identifiable information associated with those names was at risk. A full investigation is currently underway."

Epsilon says it sends more than 40 billion emails annually to customers of their more than 2,500 clients. Among those clients reportedly affected by the breach are Ameriprise Financial; Best Buy; Brookstone; Capital One; Citi; Disney Destinations; Home Shopping Network; JP Morgan Chase; Kroger; LL Bean Visa Card; Marriott Rewards; McKinsey & Company; New York & Company; Robert Half Technologies; The College Board; TiVo; US Bank and Walgreens.

Commissioner Rubenstein said his concern is that customers may receive what looks to be a legitimate e-mail from one of those companies, but it has been sent by a scammer asking for account numbers or other information that could be used for fraud. The e-mail may also direct the customer to a link of a fake website that downloads a keystroke logger or other malware or virus onto home computers.

"Even if the only data taken in this breach are email addresses, it still poses a significant risk to consumers in terms of phishing scams and other types of Internet fraud," Rubenstein said. "Consumers need to be particularly vigilant about not providing any personal information requested in an e-mail, even if it appears to be from a legitimate company they have business with. This includes Social Security numbers, account numbers, dates of birth, or other identifying information."

Attorney General Jepsen sent a letter to the company Monday asking for more information about how the breach occurred and what was being done to make sure a similar breach does not happen again.

"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.

In addition, Jepsen said he expected the company to help consumers who may be harmed by phishing scams.

"For a company such as Epsilon, which manages customer databases and regularly emails consumers of scores of companies, the security of consumer information is critical. I expect Epsilon to work with and protect any consumers harmed as a result of this breach," Jepsen said.

Assistant Attorney General Matthew Fitzsimmons is handling this matter for Jepsen.

Hackers and spammers often use e-mail to access information stored on personal computers, to spy on Internet surfing, to steal personal information and or use compromised computers to send spam to other computers. As a result, Jepsen and Rubenstein advised consumers to act immediately to protect their home computer and all e-mail accounts.

According to the Federal Trade Commission, among the steps consumers can take are:

* Install a good quality anti-virus, anti-spyware software and keep it up to date.
* Set your operating system software to download and install security patches automatically.
* If you suspect that any of your passwords have been compromised, call that company immediately to change your password.
* Don't use your e-mail address as a banking login ID or password.
*Avoid opening any attachments or downloading files from e-mails you receive.
* Don't download free software unless it is from a site that you know and trust.
* Check your "sent items" file or "outgoing" mailbox for messages you did not send.
* Take action immediately if your computer is infected. Disconnect from the Internet and scan the computer with anti-virus and anti-spyware software.

###

CONTACT: *Susan E. Kinsman, Attorney General; susan.kinsman@ct.gov; 860-808-5324; 860-478-9581 (cell)*
Claudette Carveth, Department of Consumer Protection; claudette.carveth@ct.gov; 860-713-6022