Twitter settles with FTC over data security lapses

June 24 2010, By JOELLE TESSLER , AP Technology Writer

(AP) -- Twitter has agreed to settle charges by federal regulators that it put the privacy of its users at risk by failing to protect them from data security lapses last year that let hackers access their accounts.

The Federal Trade Commission said Thursday the settlement bars Twitter from misleading consumers about its security and privacy practices and requires the start-up to establish a comprehensive information security program.

No monetary damages were assessed.

The FTC complaint said the breaches allowed hackers to gain administrative control over the online service, which lets users send brief messages called tweets to each other. According to the FTC, hackers were able to view email addresses and other private user information, gain access to user messages, reset user passwords and send phony tweets from user accounts.

At least one phony tweet was sent from the account of Fox News and another phony tweet was sent from the account of then-President-elect Barack Obama offering more than 150,000 followers a chance to win $500 in free gasoline, the FTC said.

The agency charges the incidents deceived users because Twitter's privacy policy pledged to "employ administrative, physical, and electronic measures designed to protect your information from

unauthorized access."

"When a company promises consumers that their personal information is secure, it must live up to that promise," David Vladeck, head of the FTC's Bureau of Consumer Protection, said in a statement.

One breach occurred in January 2009 after a hacker used an automated password-guessing tool to gain control of Twitter. The second breach occurred in April 2009 after a hacker broke into a Twitter employee's personal email account, which stored two passwords that were very similar to the employee's administrative password for Twitter.

The FTC said Twitter was vulnerable to these attacks because it used weak, lower case common dictionary words as administrative passwords and failed to take reasonable steps to prevent unauthorized access to its system. Such steps include prohibiting employees from storing administrative passwords in plain text in their email accounts, periodically changing administrative passwords and restricting access to administrative controls.

In a blog post, Twitter General Counsel Alexander Macgillivray said that even before the company reached the agreement with the FTC, it had already implemented many of the security practices highlighted by the agency. He added that the company quickly closed the security holes, notified affected users and disclosed what had happened in blog posts following both incidents.

Macgillivray also noted that Twitter employed fewer than 50 people when the breaches occurred.

"At the time of the incidents, we were ... in the midst of perhaps unprecedented user growth for an Internet company; and, didn't employ the security methods that we use today," the company said on Thursday.

Twitter said 45 accounts were accessed in the first incident and 10 accounts in the second incident.