Legal Sidebar

JPMorgan Data Breach Involves Information on 76 Million Households, 7 Million Small Businesses

10/23/2014

On October 7, 2014, JPMorgan Chase & Co. (JPMorgan) filed with the Securities and Exchange Commission (SEC), a statement disclosing some details of the data breach first announced in August. According to the filing, although account information was not compromised, hackers had access to information of users of Chase.com, JPMorganOnline, Chase Mobile, and JPMorgan Mobile, covering "*name, address, phone number and email address* [*information*] *– and internal JPMorgan Chase information relating to ... approximately 76 million households and 7 million small businesses.*" The company reported that it had found "*no evidence that ... account numbers, passwords, user IDs, dates of birth or Social Security numbers ... [were] compromised.*"

On its website, the JPMorgan's national bank advises customers that it has "seen no unusual fraud activity related to this incident" and that customers will not be liable for unauthorized transactions promptly reported. On a second webpage , the bank proclaims that JPMorgan believes that the attack has been stopped and that customers do not need to change their credit or debit cards or employ a credit monitoring service, but cautions customers to be on the alert for phishing scams.

JPMorgan did not provide individual customers with notice of the breach because it believed that it had no obligation to do so because no "sensitive customer information" was involved in the data breach. This means that JPMorgan apparently has complied with data breach notification standards promulgated by the federal banking regulators pursuant to the privacy provisions of the Gramm-Leach-Bliley Act (GLBA). These standards specify the contents of breach notices that must be supplied by telephone, mail, or electronic mail to all affected customers when a data breach involves "sensitive customer information." Should "sensitive customer information" be involved in a data breach, the guidelines require financial institutions, such as JPMorgan, to notify customers only if after a "reasonable investigation" the company determines that "misuse of its information about a customer has occurred or is reasonably possible."

Apparently, the JPMorgan data breach did not involve any "sensitive customer information" because "sensitive customer information" is defined to cover the types of information involved in the JPMorgan breach—names, addresses, telephone numbers, and e-mail addresses—only if combined with another item that would effectively open the way for a hacker to access a customer's account. The definition of "sensitive customer information" is:

> a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number.

Data breach notification laws in 47 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands are similarly structured. According to the National Conference of State Legislatures, they typically cover "personal information" such as name combined with Social Security Number, driver's license, state identification, account number, or something similar. Nonetheless, some state attorneys general are investigating whether JPMorgan fulfilled its requirements under the law with respect to alerting customers

of the possibility of risk from the data breach.

This is the second data breach experienced by JPMorgan in less than two years. In late 2013, the company suffered a security breach involving a debit card program offered to some state governments and involving 465,000 cards. Since then, JPMorgan has beefed up its cybersecurity program, which according to the CEO's letter to shareholders in the company's 2013 annual report, now involves 1,000 personnel and $250 million annually—with the CEO, on October 10, 2014, reportedly predicting a probable climb to $500 million annually over the next five years.

According to media reports, the Federal Bureau of Investigation and the U.S. Secret Service are conducting criminal investigations into the attacks. Reportedly, they are looking into whether hackers using the same I.P. (Internet Protocol) address attempted to hack into other financial institutions. They also may be trying to identify the motives behind the hacking and determining whether there is any link to the U.S-led sanctions against Russia.

Posted at 10/23/2014 09:17 AM by M. Maureen Murphy | Share Sidebar

Category: Banking

Related Policy Issue(s): Financial Market Regulation, Consumer Protection