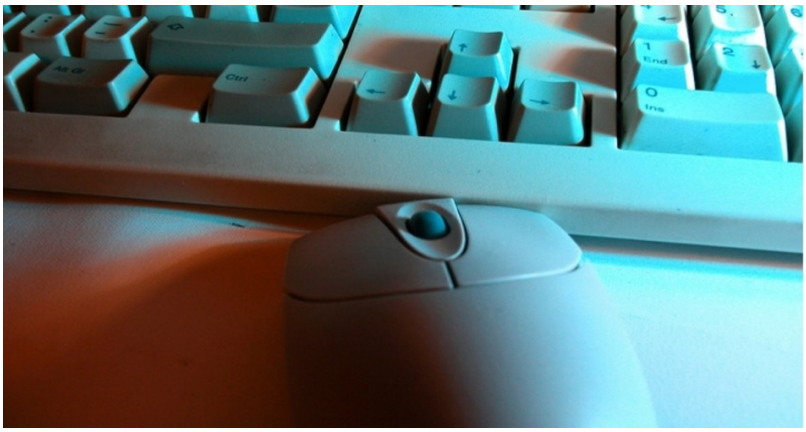
Written by **Kurt Hyde** on October 6, 2014

Data Breach at JPMorgan Chase Affected 76 Million Households — Were Government Guidelines Partly to Blame?



JPMorgan Chase filed an 8-K report with the Securities and Exchange Commission (SEC) Thursday explaining the extent of the cyberattack first reported in July. The 8-K report says:

> • User contact information — name, address, phone number and email address — and internal JPMorgan Chase information relating to such users have been compromised.

• The compromised data impacts approximately 76 million households and 7 million small businesses.

• However, there is no evidence that account information for such affected customers — account numbers, passwords, user IDs, dates of birth or Social Security numbers — was compromised during this attack.

The report went on to say that as of the filing date the company had not seen any unusual customer fraud related to the incident.

Reaction by computer professionals to this data breach has ranged from relief that there's no evidence of consumer fraud to concern that such a breach could have occurred despite the highly sophisticated security at JPMorgan Chase, as well as other financial institutions. A breach such as this implies highly skilled intruders. It even invites the question of did they succeed unnoticed and then deliberately leave some evidence of the breach in order to measure the ability to detect the breach and the reaction to it?

Consumers are being warned that they might be vulnerable to phishing scams via phone or e-mail and are advised not to give their passwords to these people.

But the one area of concern that is absent from the mainstream media is the role played by government agencies in increasing the vulnerability of computers, not the least of which was unconstitutional spending by the Eisenhower and subsequent administrations to finance development of the Internet. Research in the private sector was already developing computer networking that was inherently more secure, but the government-sponsored product became the standard. Had the private sector won, customers would have the option of different network technologies. Additionally, there would be no dispute today about who should govern the computer networks. They'd be privately owned.

A previous article in *The New American* online has dealt with these topics and others, such as affirmative action rules that mandate hiring priorities for minorities over many Americans, even if the prospective employees come from terrorist-exporting nations.

It is believed by some that this breach was caused by someone getting one or more passwords via social engineering. If so, the federal government may have had a hand in making it easier for an unauthorized person to get them.

The federal government has been leading the way in encouraging what they call strong passwords. Computer passwords should have some strength, but recent federal edicts have gone over the top. The June 2013 implementation of overly strong passwords at the Defense Finance and Accounting Service (DFAS) for access by military people is a case in point. The passwords had to be a minimum of 15 characters with at least two uppercase characters, at least two lowercase letters, at least two numbers, and at least two special characters (!, @, #, $, -, *, =, _). On top of that, the passwords expired every 60 days. These ridiculous rules were eased slightly in May of 2014.

What happens when so-called strong passwords are actually overly complex? Most computer users write down their passwords, but they keep them tucked away. When passwords are overly complex, even the computer professionals with considerably higher IQs are forced to write them down, and possibly even leave them lying around on their desks at work because they are referenced so often. Passers-by during the day and cleaning crews that have access to offices after work may find these passwords easily.

Overly complex passwords lead to more phone calls for password resets. A typical means of authentication over the phone is someone's Social Security number and birthdate. Of course, that information isn't really a secret. People use these numbers so frequently that they are known at multiple call centers overseas as well as in the United States. When overly complex passwords lead to frequent calls for password resets, the user's Social Security number and birthdate become the real password. If calls for password resets are common, a password reset request by a hacker who knows someone's Social Security number and birthdate won't even raise an eyebrow.

This recent data breach needs to be investigated thoroughly. Computer users should be on the lookout for phishing schemes. It is also time to examine what role the federal government may have played in enabling this data breach.