

Data Breach at JP Morgan Chase Could Impact Millions

August 28, 2014 - JP Morgan Chase is working with federal law enforcement authorities to determine the extent of a data breach caused by hackers. At this point, the bank has said little about what data was stolen but Bloomberg news is reporting that it involved gigabytes of information and that customer and employee data is what the hackers targeted.

Tweet

```
(function() {  
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];  
s.type = 'text/javascript';  
s.src = 'http://widgets.digg.com/buttons.js';  
s1.parentNode.insertBefore(s, s1);  
})();
```

```
(function() {  
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;  
po.src = 'https://apis.google.com/js/plusone.js';  
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);  
})();
```

Federal authorities seem to believe that the breach was caused by Russian hackers; perhaps in retaliation for American sanctions on Russia for their invasion of the Ukraine.

Over the past two months, malicious software (malware) was discovered on two overseas servers belonging to Chase. This malware was capable of stealing data and compromising the company's network. This most recent attack of Chase's computer network may very well have begun the same way.

The FBI has not yet been able to determine exactly what data was stolen or how many people will be impacted. And Chase bank hasn't even come out and said that the company was a target of the attack. But both customers and employees of Chase should take some precautions.

Anyone who accesses their accounts online should begin checking them regularly for issues. Since the data stolen may have included both bank account and credit account numbers, customers of the bank should be monitoring all of their accounts.

In addition to this, the data that was stolen may very well have included social security numbers. This means that Chase customers should be considering additional options. These include using a service designed to restore your identity if you are victimized, placing a fraud alert on your credit file or placing a freeze on your credit file.

As more information on the breach becomes available, ACCESS will publish it.

by Jim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, [click here](#).

Registration is easy and free.

Follow me on Twitter:

Follow ACCESS