JPMORGAN'S FORM 8-K TO INVESTORS: WE'VE BEEN HACK-MAPPED!

JPMorgan's Form 8-K filed on Thursday with the Securities and Exchange Commission advises:

> On October 2, 2014, JPMorgan Chase & Co. ("JPMorgan Chase" or the "Firm") updated information for its customers, on its Chase.com and JPMorganOnline websites and on the Chase and J.P. Morgan mobile applications, about the previously disclosed cyberattack against the Firm. The Firm disclosed that:
>
> • 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.
>
> • As of such date, the Firm continues not to have seen any unusual customer fraud related to this incident.
>
> • JPMorgan Chase customers are not liable for unauthorized transactions on their account that they promptly alert

> the Firm to.
>
> The Firm continues to vigilantly monitor the situation and is continuing to investigate the matter. In addition, the Firm is fully cooperating with government agencies in connection with their investigations.

According to ZDNet, a forensic security firm suggests the bank's users' accounts are now at greater risk of compromise and that password changes and two-factor authentication should be implemented to address the risk.

However, the 8-K's wording indicates a different security risk altogether as the users' passwords and Social Security numbers are not compromised.

The disclosure of information compromised combined with earlier reporting about the breach more closely matches a description of that collected by National Security Agency's TREASURE MAP intelligence collection program. TREASURE MAP gathered information about networks including nodes, but not data created by users at the end nodes of the network. The application delineated the path to the ends. and physical ends, not merely virtual ends of the network.

The items at risk according to JPMorgan's filing are metadata components – name, address, phone number and email address. As the Guardian's guide to metadata explains – beginning with telephone and cellphone numbers, and email addresses – the following additional metadata can be obtained with adequate access to JPMorgan's servers and network:

Email metadata:

- sender's name, email and IP address
- recipient's name and email address
- server transfer information

- date, time and timezone
- unique identifier of email and related emails
- content type and encoding
- mail client login records with IP address
- mail client header formats
- priority and categories
- subject of email
- status of the email
- read receipt request

Cellphone metadata:

- phone
- phone number of every caller
- unique serial numbers of phones involved
- time of call
- duration of call
- location of each participant
- telephone calling card numbers

All of this could be linked to a real name and a real, physical address also contained in JPMorgan's affected database. With these items, an entity can begin to cross-match physical locations against behaviors.

Consider, too, that JPMorgan's Form 8-K does NOT tell us definitively is whether information regarding assets in customer accounts has been breached as well. However, the 8-K says, "internal JPMorgan Chase information relating to such users" has been compromised; does this mean that not only value of assets, but types of assets and transaction records have been accessed?

Imagine being able to select specific customers, locating them physically, and then narrowing targeting even further based on their asset

types or value.

What could be done with this information? Let's speculate on applications:

> – Customers holding specific assets or majority positions can be monitored for potential trading activity, so that trades can be front-run ahead of a major ownership or market position change;
>
> – Identified customers can be physically threatened about assets in their holdings, or about activity that may affect a market;
>
> – Information about customers' positions can be used to damage markets and inflict economic injury to individuals or groups of people.
>
> – At volume, information about cash flows of ALL customers in aggregate could be used for front-running.

There are other potential uses for such information if one continues this line of speculation.

Clearly JPMorgan felt there was a material risk to investors obligating them to file a Form 8-K – not every publicly-held corporation's security breach has been reported, in contrast. Target, Home Depot, even NASDAQ cyber security breaches are examples in which the firm did not generate 8-K reports.

While a handful of other major firms now publish Form 8-K notifications of major breaches, JPMorgan has not previously done so. This cannot possibly be the first or only cyber security breach this financial institution has faced. What makes a critical difference is that this breach poses a threat of unknown nature and magnitude; no evidence of fraud or unauthorized activity has been detected, but the potential damage to investors may happen outside JPMorgan accounts, to markets as a whole, impacting holders of JPMorgan's stock (NYSE:JPM) as well as its customers.

Does the nature of this breach as an intelligence gathering operation pose such a threat to its investors that JPMorgan had no choice but to make this disclosure?

And what does the pattern of JPMorgan's customers' asset and cash flows look like in the wake of this 8-K?

It's worth noting, too, the change JPMorgan's stock valuation during the period following issuance of their dividend and the release of the Form 8-K before Friday morning. What shifted the stock back up more than a dollar per share?