MAPPING TREASURE: LOOKING BEYOND THE YIELD OF TRADITIONAL INSIDER TRADING

[graphic: Money by Kevin Dooley, via Flickr]

A former SAC hedge fund manager, who cooperated with law enforcement, avoided a prison sentence this week after the FBI's investigation into insider trading found criminal activities. It's a rather typical story in which persons unfairly benefited from information they would not otherwise have access to outside their work as traders. Six persons were ultimately convicted in connection with this case.

A fresh spin on insider trading also made news this week, when the SEC filed a lawsuit against two Capital One fraud investigators who made 1800 percent on their investment over three years, based on their use of a Capital One credit card user database.

The two investigators, Bonan Huang and Nan Huang, grew an investment of $147,300 to $2.8 million based on thousands of searches across a database comprised of credit card customer transactions. Noting the volume of use of credit

cards at a particular fast food company, they bought and traded the company's stock based on this data.

Over time they made similar stock trades based on transactional volume and other publicly available news about three different companies.

Had the database been one for sale by a company rather than their employer's proprietary database, the Huangs would have been lauded as investment rock stars. But because the method they used "misappropriates confidential information for securities trading purposes, in breach of a duty owed to the source of the information," the two men are being sued for insider trading.

The Huangs' trading experience gives pause when one considers the value of metadata, and of the data breach at JP Morgan Chase this past year.

Metadata can offer a volume of transactional activity, though it will not disclose the value of a transaction. Imagine smartphones indicating they are being used at particular devices – point-of-sale devices – at any retailer, from fast food to hard lines. An uptick in overall activity at a specific retailer indicates greater volume of business, the data fresher than that reported in a 10-Q report filed publicly with the SEC. What could an investor do with this kind of data? One could imagine success not much different than the Huangs experienced, provided they also understood other publicly available information about the retailers under observation.

Imagine the data created by cashflow movements in and out of ~83 million bank and investment accounts at a corporation like JP Morgan Chase. What could investors do with this information? The kind of information obtained by the hack disclosed in 2014 may have included account activity:

> 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.

JPMC stressed passwords were not leaked. The data available to the hackers, though, was not very dissimilar from that gleaned by the NSA's TREASURE MAP program – identities, locations, and "internal JPMorgan Chase information" included.

But perhaps the hacker(s) didn't intend to break into accounts; perhaps instead they merely wanted access to real-time data about financial movements, especially in and out of key accounts, or across the entire enterprise at scale. Or perhaps even early peeks into startups and IPOs underwritten by JPMC, some of them based on technology patent awards.

What's interesting, too, is the fuzziness of the government's response as to the identity of culprits responsible for the JPMC data hack. In August, "two people familiar with the probe" discussed suspicions that Russia was behind

hacking of JPMC. Yet in October, subsequent reporting about the hack doesn’t mention Russia at all, discussing instead the possibility of phishing attacks.

In contrast, the public was assured firmly in a relatively brief period of time after data leaked that Sony Pictures Entertainment was hacked by North Korea (though the evidence offered to date is sketchy). Is the government still looking for hackers who might have benefited from JPMC data, without actually touching any of the account holders’ assets?

Perhaps they should be looking for parties with better than 1800 percent yield on investments.