Our Perspectives:
Commentary on the economy & regulatory policies affecting financial companies

Barnett Sivon & Natter P.C.
ATTORNEYS at LAW
WASHINGTON, DC

# Cyber Threats to Financial Services*

Bob Barnett

March, 2014

> No area of emerging risk is more important today than the cyber threats that are increasingly common in our interconnected environment.
>
> – Thomas Curry, March 4, 2014

Recent attacks by third parties have resulted in losses of $45 million in cash from ATMs and acquisition of credit card information about hundreds of thousands of customers from some retail stores. The second wave of losses from the credit cards has begun as the information captured in the hacks has begun to be used to acquire other goods and services, and probably to capture other card information. There is no reason to believe that these kinds of attacks are not already working in other sites, and in more sophisticated form, will be used in the near future in more varied environments to acquire, illegally, cash or other assets and customer information.

The attacks can come in a number of different forms. Some are direct attacks on a company's site, overloading it so that it cannot perform its normal operations. Those attacks seem to arrive without warning and can overwhelm a network quickly; nevertheless, there are security systems that can alleviate those attacks, and firms that consider themselves particularly vulnerable to them can establish barriers that will thwart the worst results.

Other direct cyber attacks can attempt to bypass firewalls in the financial firm's own security systems and access either assets or customer information held by the firm. Financial firms hold a treasure trove of valuable customer information that can provide individuals or firms that obtain it direct access to things of value that can be used either to harm the firm or the customers or to benefit the hackers. Sometimes the result is both — benefit to the hackers and losses and reputational damage to the financial firm.

The hacker can, of course, once in the files of the firm, consider hacking into the customers of the firm through the data exchanges that occur between the firm and its customers. Often bypasses around security or one to one links through security exist in order to improve the efficiency of the performance of the relationship between the bank and the customer. While these channels do make it easier for the vendor to carry out its

*The information contained in this newsletter does not constitute legal advice. This newsletter is intended for educational and informational purposes only.

job, they can create weaknesses in the security between the two firms on which bad guys can capitalize. Even if such bypasses do not exist, the difficulty in breaching the wall between the firm and the customer is often less than attacking either directly.

Sometimes the financial firm's firewalls are difficult to breach, and the hacker is then forced to find other ways to access the firm's information. Access through third party vendors used by the firm is one obvious approach, and the one used successfully in some of the retail site breaches. Vendors often do not have the same high level of security that the financial firm itself has, and the amount of resources assigned to security is often not as great as that assigned to security in the financial firm. Therefore, breaching is easier.

While so far the hackers have been driven by, greed, for lack of a better word,[1] there may come a time when the goal is the corruption or destabilizing of an institution or the payment system or some similar slice of the network on which the financial world runs.[2] That makes security in the financial system vital not only for P&L purposes, but for national security.

Cloud computing has become common, i.e., the use of servers, accessible through the Internet, to provide computing and other IT services to firms. That innovation is cost effective for many financial firms in many contexts and so is irresistible.

Cloud computing by its nature creates substantial cyber risks. The firewalls between the server found on the Internet and the financial firm must be clear and unequivocal to the server, and if the server finds it costly to adopt the protocols needed to comport with the rules imposed upon financial firms with respect, say, to customer privacy, the firewall may not be tight. Or the server may have other customers in its cloud and has as a procedure capturing and performing tasks with respect to data of more than one firm at one time. This creates the risk that the data will not remain secure, of course, and the further risk that entrance and exit to the commingling may present opportunities to the hacker.

As the saying in the industry goes, you can outsource the work but you can't outsource the risk. Larger firms are more apt to be able to impose upon the cloud servers the kinds of protocols necessary to maintain their own and their customer's security. Smaller firms may not have the same leverage.

Certain firms are more susceptible to cyber attacks. Larger financial firms, of course, present larger, perhaps potentially more lucrative targets to the cyber criminal, so they are natural targets. As such, and having the resources they do, they have developed the best set of protections against cyber attacks. Criminals, therefore, may find it to their advantage to focus on those that do not have the same expertise, even though the returns on any successful hack may be smaller.

Smaller firms such as community banks or even many regional banks do not have the same IT and security expertise in house as do large firms, and often have only a very limited amount of resources that can be placed against that particular risk. They are logical targets for cyber attacks, assuming the hackers can devise a scheme that will make the hack worth their time. Criminals are very creative, so it seems clear that they will devise appropriate schemes.

No firms, regardless of size, however, are immune to clever cyber criminals. While it is xenophobic to believe that firms are more cautious with third party data in the U.S. than elsewhere, there is a concern among many that firewalls may be more easily breached in some foreign countries. At the same time, some

[1] Thank you, Gordon Gekko.

[2] The U.S. Navy records have been hacked, by Iran no less, because of an insufficiency in the contract between the Navy and a vendor — i.e., the contract failed to designate who was supposed to establish the firewalls which would have prevented the hacking.

of the foreign firms offer terms and conditions that make their product seem very desirable, and therefore firms are tempted to take advantage of that, even if due diligence on such firms is difficult, if not impossible, to conduct.

As Comptroller Curry has said, "Third party service providers and subcontractors of third parties that operate in foreign jurisdictions present unique problems." Those problems are not limited to risks that are undertaken by the firm, but the difficulty in determining the effect of local laws on creation, storage, transmission, and ownership of data.

The regulators have become very aware of the risks of cyber criminals attacking one or more parts of the payments system, and will be expecting firms they regulate to treat that risk as seriously as the risk it creates demands. That will include not only robust due diligence and careful monitoring of the third party vendors in cases in which they are used, but similar intense review of a firm's security in light of the creativity shown by cyber criminals.

*Bob Barnett is a partner with the law firm of* ***Barnett Sivon & Natter, P.C.***