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

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

CFPB and Potential Breaches of its Data Security Systems*

Bob Barnett

December, 2014

It is not the normal thing for a company to ask the Federal Government to agree to make it whole should the Federal Government make a mistake that harms it. There is a doctrine of sovereign immunity that protects the government from most lawsuits. But there are times when that general rule should be overridden. The latest expansion of the HMDA rules as proposed by the Consumer Financial Protection Bureau combined with the harsh judgment of the Bureau's ability to secure the data it collects may be one of those times.

Weaknesses reported in CFPB security systems

Two government agencies have very recently independently found major weaknesses in the data collection security systems of the CFPB.[1] Those weaknesses included a conclusion by the GAO that the "CFPB lacks written procedures for its data intake process, including for evaluating whether statutory restrictions related to collecting personally identifiable financial information apply to large-scale data collections...and assessing and managing privacy risks of these collections."[2] It also said that the Bureau has not created a comprehensive privacy plan, and failed to meet certain key elements necessary for implementing the National Institute of Standards and Technology guidance on risk assessments and remedial action plans. Similarly, the Office of Inspector General of the Federal Reserve and the CFPB found weaknesses that it did not detail publicly, but publicly did state that the CFPB needed to enhance security with regard to system and information integrity, configuration management, contingency planning, and incident response.

These weaknesses exist notwithstanding the major effort currently underway by the President to improve information security and privacy management practices.[3] The memorandum issued by the President identifies administration priorities and establishes new policy guidelines to improve the secure federal information security process. That robust effort and its requirements apply to the CFPB, and, at this juncture, but unfortunately, it seems clear that the Bureau systems do not comply with these various guidelines and policies.

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

[1]Office of Inspector General: Federal Reserve and CFPB, Security Control Review of the CFPB's Cloud Computing-Based General Support System (July 17, 2014) ***Some Privacy and Security Procedures for Data Collection Should Continue Being Enhanced***; Government Accountability Office, Consumer Financial Protection Bureau: GAO-14-758 (September 2014).

[2]Id. at 64.

[3]Executive Office of the President, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*, (October 3, 2014).

The Bureau proposal with respect to HMDA data

In its most recent proposal to expand reporting under HMDA, the Bureau proposes to add three dozen new data points to those it is already collecting. The addition of many of these will make it relatively easy for third parties to identify individuals and their personal confidential financial information directly from the data collected. Recognizing that, the Bureau says it will, for the time being, redact most of these kinds of data from data that becomes publicly available. That is helpful, assuming that the systems work correctly at the CFPB, but is not sufficient for all possible harm to the companies supplying the data.

The Bureau also plans to permit access to this expanded store of data to third parties, without clarifying in the proposal what parameters it might place around the data made available or the credibility or trustworthiness of the third parties who will have access. For example, no rules have been established for who may conduct research from the data, how responsible such researchers might be, what peer review (if any) would be required of the researchers or their reports, etc. In addition, the Bureau has not said that any rules it might establish (should it decide to establish any) would be subject to notice and comment.

This is not a modest amount of data that would be subject to such research. In 2012, there were about 19 million loans reported under HMDA. Adding 37 new data points to the already existing large number, as well as such provisions in the proposal as the one to require that HELOC data be reported, will expand the reported data significantly.

Risks from weaknesses in CFPB data security systems

While companies might have some protection from lawsuits from an individual if a breach at the Bureau unwittingly reveals personal confidential information about a consumer in violation of privacy laws (the old "the government made me do it" defense), that is not clear. In addition, that will not, unfortunately, prevent the media from using the exposure of customer information in yet another story in which the reputation of banks will take a hit. It will also spread a chill among the customers that information they provide in confidence to their financial institutions will not be treated confidentially, and at some point, may be available to the public. More important, it will increase the risk of fraud and identity theft for our customers.

Beyond the immediate problem that this presents, however, is yet another risk that is harder to quantify, but with each passing day seems to be more of a problem. The ability of third parties, whether state sponsored or rogue groups of self-identified heroes, to hack into systems of U.S. institutions grows by the day. While those in which retail establishments or financial institutions have been the targets get most of the media attention, it is instructive to realize that the security systems of the CIA, White House, Navy, and other government institutions have also been subject to unauthorized intrusions. The ability of persons interested in intruding into systems seems lately to be a step ahead of the protections that have been designed to prevent their entry.[4]

Many hacks have occurred indirectly when the intrusion enters through a third party vendor. At this point, it is not clear to what extent the CFPB uses such third parties or how successful the protections the Bureau uses are to protect themselves from indirect intrusion through their vendors. That, of course, compounds the problems for those reporting data.

[4]During testimony before the House Intelligence Committee recently, Admiral Rogers, director of the National Security Agency, said that the U.S. can expect in the next decade a concerted foreign-based cyber-attack on the electronic industrial control systems that operate such facilities as the nation's power grid, nuclear power plants, air traffic control systems, etc. Hacking into the CFPB should be relatively easy if they can do that.

Finally, the real danger could be that there is a sufficient connection between the Bureau and the reporting entities that a hacker could move backwards into the reporting companies once they had entered the Bureau. It is not clear that there is such a connection but should there be one, or if one is created, the risk of exposing the reporting entity itself to the intrusion would be magnified.

Need for protection from damages caused by intrusion into CFPB systems

One could argue that the collection of HMDA data[5] by the Bureau carries with it an implication that the data will be protected and will not become available to unauthorized third parties. If so, there may be ways for companies damaged by the effects of intrusions to assert a claim.[6] Litigation, of course, is expensive, particularly against an adversary with unlimited funds, and, in addition, against one that regulates and supervises your company.

A better way would be for data collection of this magnitude to be conducted under a protocol that would include a careful delineation of the rights of the parties in the case of an unauthorized intrusion into the Bureau that either (a) permits access to otherwise confidential information that has been collected, or (b) permits access into the systems of the reporter itself, thereby causing extraordinary damage. Those rights, memorialized in a specific agreement with each reporter, would include payment of appropriate compensation in case these intrusions caused demonstrable damage. Basically, this means a non-disclosure and a hold harmless agreement between the Bureau and each reporter.

While the executive branch and its departments and independent agencies may well have the authority to enter into such agreements, they may feel more comfortable if Congress directs them to do so. Either way, there is the need for such agreements in the current environment.

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

[5]This would be true of collection of other data by other agencies also.
[6]See, for example, possibilities under 28 U.S.C. sec. 1346(a)(2).