

March 28, 2006

IS IT FAIR TO ENFORCE THE INFORMATION SECURITY GUIDELINES THROUGH CIVIL MONEY PENALTIES?

**Peter Heyward
Venable LLP¹
Washington, D.C.**

Introduction

There's a funny scene in the movie "Ghostbusters," when Bill Murray, as spook eradicator Peter Venkman, responds to a call from client and romantic interest Dana Barrett (Sigourney Weaver), who has reported disturbing supernatural phenomena in her apartment.

When Venkman arrives at her door, it is obvious that Dana is no longer herself: She appears sexily attired in a revealing dress and, drawing Venkman into her bedroom announces: "I am Zuul, the Gatekeeper . . . Do you want this body? Take me now!"

Venkman demurs, explaining: "I make it a rule never to get involved with possessed people." But as Dana, continuing to come on strong, pulls him down on her bed, he allows: "Actually, it's more of a guideline than a rule."

The line gets a big laugh, because everyone understands that you risk serious punishment for violating a "rule," whereas a "guideline" can be flouted with impunity.² This understanding of the difference between a rule and a guideline may explain the lively reaction at a morning session during the Fall meeting of the Banking Law

¹ The author is a partner in the Financial Services Group of Venable, LLP, based in Washington, D.C. The opinions expressed in this article do not necessarily reflect the views of other partners or employees of Venable LLP, or any of its clients.

² OK, maybe not with impunity, but at most with some bad publicity and, perhaps, an admonition to do better the next time. A case in point: the short-lived reaction to recent violations of the Fourth Guideline to the U.S. Constitution (recommending that law enforcement authorities "consider whether it is appropriate" to obtain a warrant before conducting wire taps or intercepting e-mail).

Committee, when a panelist representing one of the federal banking agencies reported that First Horizon Loan Corporation, a national bank operating subsidiary,³ had been tagged with a substantial civil money penalty for violations of the Interagency Guidelines Establishing Standards for Safeguarding Customer Information (the "Information Security Guidelines").⁴ Despite the early hour, many a dozing lawyer – including me - jerked awake at that announcement. How could an agency impose a CMP for violating *guidelines*?

This question stemmed, at least in my case, from the belief that "guidelines" are inherently not the type of agency pronouncement that should be enforceable by civil money penalties or other punitive sanctions. Guidelines are generally drafted in broad, general terms, so it simply seems unfair to impose penalties when the supposedly prohibited conduct is not clearly spelled out.

Although the First Horizon case is not clear on the point, I understand that the legal theory on which the OCC relied was that First Horizon violated a "regulation," thereby becoming subject to first tier civil money penalties. 12 U.S.C. §1818(i)(2)(A)(i). The legitimacy of this approach, as a policy matter if not as a legal one, seems to me to be questionable. On the other hand, considering the Information Security Guidelines as they existed at the time of First Horizon's alleged misconduct, I believe that the OCC's action could have been justified both legally and as a policy matter, provided one makes the crucial assumption that First Horizon's conduct was "reckless" and was either part of a pattern of misconduct, caused or was likely to cause more than a minimal loss to the

³ *In the Matter of First Horizon Home Loan Corporation*, Stipulation and Consent Order for Civil Money Penalty, OCC Enforcement Decision 2005-78, June 30, 2005.

⁴ These Guidelines, adopted by all the federal banking agencies, are codified at 12 CFR Part 30, Appendix B (national banks); 12 CFR Part 208, Appendix D-2 (state member banks); 12 CFR Part 364, Appendix B (state nonmember banks); and 12 CFR Part 570, Appendix B (thrift institutions).

institution (other than the CMP itself!), or resulted in pecuniary gain or other benefit to First Horizon.⁵ In the discussion that follows, I will try to explain these conclusions.

Discussion

First Horizon is a mortgage lender and operating subsidiary of First Tennessee Bank National Association, a subsidiary of financial holding company First Horizon National Corporation of Memphis, Tennessee. Without admitting or denying wrongdoing, it consented to the issuance of a civil money penalty in the amount of \$180,000 for "violations of the customer information security protections" set forth in the Information Security Guidelines. The Consent Order reveals few of the underlying facts, but it was reported that the penalty related to an incident in November 2004 in which a customer found loan files for approximately 120 people in a dumpster outside a First Horizon office in Fairfax, Virginia.⁶ The company reportedly claimed that movers mishandled the information while the office was being moved, and that it had promptly notified the affected customers and the OCC when the problem was discovered.

The Information Security Guidelines were promulgated by the banking agencies under the authority of Sections 501 and 505(b) of the Gramm-Leach-Bliley Act ("GLBA"), codified at 15 U.S.C. §§6801 and 6805(b), respectively, and Section 39 of the Federal Deposit Insurance Act (the "FDI Act"), codified at 12 U.S.C. §1831p-1. Section 501(b) requires financial regulators to establish standards for the entities under their jurisdiction to protect the confidentiality of customers' records and information, while

⁵These are, of course, the standards for imposing second tier civil money penalties based on engaging in an unsafe or unsound practice in conducting the affairs of the institution. 12 U.S.C. §1818(i)(2)(B). I emphasize that I have no personal knowledge of the facts in the First Horizon case beyond what has been publicly reported, and I make no judgment that First Horizon's conduct in fact satisfied the statutory standard for the imposition of either first or second tier CMPs.

⁶ Davenport, *Breaches, Credibility, And Agencies: With data security 'the new BSA,' banks need to adapt*, American Banker, July 28, 2005.

Section 505(b) directs the *banking* regulators to implement the information security standards mandated under Section 501 "in the same manner, to the extent practicable," as the safety and soundness standards prescribed pursuant to Section 39 of the FDI Act. It is noteworthy that Section 505(b) directs the regulators responsible for financial entities other than banks – the Securities and Exchange Commission, state insurance regulators, and the Federal Trade Commission – to implement the information security standards “by rule.” 15 U.S.C. §6805(b)(2).

Section 39 directed the banking agencies to prescribe various standards for safety and soundness, but it gave them the option to act by "regulation or guideline." 12 U.S.C. §1831p-1(d)(1). As it happens, by the time GLBA was enacted in 1999, the banking agencies had elected to prescribe *all* of the safety and soundness standards required by Section 39 by guideline rather than regulation. 60 Fed. Reg. 35674 (July 10, 1995). It therefore seems clear that Congress intended the information security provisions of GLBA to be implemented for banks through the flexible mechanism of guidelines, rather than by regulations. The deliberateness of Congress's choice is underscored by its decision to require that the standards be implemented “by rule” for financial institutions other than banks.

There is also some evidence in Section 39 for a preference for an enforcement mechanism that emphasizes corrective action rather than penalties: The provision authorizes the banking regulators to require a bank that fails to comply with a safety and soundness guideline to submit a corrective plan. Should the bank fail to submit or implement such a plan, the agencies are authorized to take various measures – restricting

asset growth, increasing capital, limiting interest rates – that focus on restoring the erring bank to financial soundness.

Nevertheless, it is hard to argue that Section 39 *precludes* the banking agencies from taking other enforcement actions. Subsection (g) expressly states that “the authority granted by this section is in addition to any other authority of the Federal banking agencies.” 12 U.S.C. §1831p-1(g). The banking agencies reaffirmed this principle in the Safety and Soundness Guidelines that they promulgated in 1995:

Neither Section 39 nor these Guidelines in any way limit the authority of the agencies to address unsafe or unsound practices, violations of law, unsafe or unsound conditions, or other practices. Actions under section 39 and these Guidelines may be taken independently of, in conjunction with, or in addition to any other enforcement action available to the agencies.

12 CFR Part 30, Appendix A, Part I.A (Preservation of Existing Authority) (Provision applicable to national banks).

Therefore, while it seems clear that Congress intended the banking agencies to employ guidelines rather than rules or regulations in implementing the information security provisions of GLBA, one must assume that Congress was also aware of this reservation of authority in Section 39. In other words, there is no necessary implication that Congress intended the banking regulators to refrain from using their usual supervisory tools in appropriate circumstances to enforce the Information Security Guidelines.

This evidently is the banking agencies' position. They included in the Information Security Guidelines a clause preserving their other enforcement authorities that is virtually identical to the preservation-of-authority provision in the Safety and Soundness Guidelines. *See* Interagency Guidelines Establishing Standards for Safeguarding

Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 65 Fed. Reg. 39481 (June 26, 2000). The Preservation of Authority provision was included in the final version of the Information Security Guidelines in 2001, and has remained in them ever since.

Still, federal banking laws nowhere refer to the imposition of civil money penalties for violating “guidelines.” To find a legal basis for assessing a first tier CMP against First Horizon, one must identify a violation of a "law or regulation." 12 U.S.C. §1818(i)(2)(A)(i)⁷. Based on discussions with a lawyer familiar with the First Horizon matter, the OCC's theory was that the Information Security Guidelines constituted a "regulation" for purposes of the civil money penalty provisions of Section 1818, and that First Horizon had violated the regulation, presumably (if the news reports were accurate) by improperly disposing of sensitive customer records.

The Information Security Guidelines do, in fact, meet at least one important requisite for being treated as a binding regulation under administrative law principles: they were issued after public notice and comment in June 2000 before being adopted in final form in late January 2001.⁸ This is not the case for all interagency guidance documents.⁹ Moreover, an agency lawyer has argued that, by avoiding the "regulation" label for the Information Security Guidelines, the banking agencies have greater flexibility with respect to remedial action in the event of a violation, which is desirable

⁷ It is my understanding that there was no basis for alleging any of the other predicates for a first tier CMP, namely a violation of a final order, temporary order, condition imposed in writing by, or written agreement with, the OCC (as First Horizon's "appropriate federal banking agency"). 12 U.S.C. §1818(i)(2)(A)(ii) – (iv).

⁸ The Agencies published the proposed Guidelines on June 26, 2000 (65 FR 39472); their adoption in final form was announced in the Federal Register on February 1, 2001 (66 FR 8616).

⁹ For example, the Interagency Advisory in Influenza Pandemic Preparedness issued on March 15, 2006. Presumably, we won't be seeing any CMPs imposed on banks for failing to keep the washroom well stocked with clean towels.

from both the agencies' and the banks' perspectives. Under Section 39 of the FDI Act, 12 U.S.C. §1831p-1, if the Guidelines were a "regulation," the appropriate federal banking agency would have no choice but to require an acceptable corrective plan upon finding that an institution had failed to comply, whereas the agency is permitted, but not required to request such a plan if the Guidelines are "guidelines."¹⁰

I find this approach questionable for several reasons. First, as discussed above, Congress, in GLBA, may reasonably be understood to have directed the banking agencies to implement the Information Security Guidelines by guideline rather than by regulation. I don't believe that this statutory mandate is fulfilled by implementing standards that are called "guidelines" but treated as *regulations* for enforcement purposes. A second objection, related to the first, is that it is inconsistent to assert that the Information Security Guidelines are enforceable for civil money penalty purposes as "regulations," but should not be treated as "regulations" for purposes of the provisions of Section 39 of the FDI Act. It is not very convincing to argue that this approach avoids forcing the agencies to impose a corrective plan for every violation of the Guidelines, which would be the case (it is asserted), if the Information Security Guidelines were treated as

¹⁰ The statute provides that when a bank fails to comply with a safety and soundness *guideline*, the banking agency "may" require the bank to submit an acceptable corrective plan within a specified deadline. 12 U.S.C. §1831p-1(e)(1)(A)(ii). The statute contemplated a slightly different consequence of failing to meet a safety and soundness standard that was imposed by *regulation* rather than guideline. In that case, the statute stated that the appropriate banking agency "shall require" the bank to submit a corrective plan. 12 U.S.C. §1831p-1(e)(1)(A)(i). In any event, once a corrective plan has been required (whether the requirement was mandatory or discretionary), the consequences of failing to submit such a plan or to implement it in any material respect, are the same: the agency "shall require" the bank to correct the deficiency and "may" take on or more of the following steps until the deficiency has been corrected:

- (i) restrict the bank's asset growth (12 U.S.C. §1831p-1(e)(2)(B)(i));
- (ii) require the bank to increase its ratio of tangible equity to assets (12 U.S.C. §1831p-1(e)(2)(B)(ii));
- (iii) restrict the interest rates that the bank pays on deposits to those prevailing in the bank's region (12 U.S.C. §1831p-1(e)(2)(B)(iii)); or
- (iv) require the bank to take "any other action that the agency determines will better carry out the purpose of" the prompt corrective action provisions codified at 12 U.S.C. §1831o ((12 U.S.C. §1831p-1(e)(2)(B)(iv)).

regulations under Section 39. I note that the civil money penalty provisions of Section 1818 also speak in mandatory terms, indicating that a bank which violates a law or regulation "*shall* forfeit and pay" a penalty. 12 U.S.C. §1818(i)(2)(A) (emphasis added) Yet the banking agencies do not feel compelled (nor should they) to impose a CMP for every violation by a bank, however trivial or inadvertent. Finally, and not least, it behooves the banking agencies to say what they mean. There is a "truth-in-labelling" problem with calling something a "guideline" but enforcing it like a "regulation."

In sum, in my judgment, the First Horizon civil money penalty can be justified, if at all, only if it meets the more stringent standards that apply to second tier CMPs for engaging in unsafe or unsound practices. The authority to impose civil money penalties on banks and IAPs for “recklessly” engaging in “an unsafe and unsound practice” has been part of the agencies’ enforcement arsenal since an amendment to that effect was made to the FDI Act in the Financial Institutions Reform, Recovery and Enforcement Act of 1989. Pub. L. 101-73, §907(a), codified at 12 U.S.C. §1818(i)(2)(B). The banking agencies clearly view the Information Security Guidelines as a statement of what constitutes “safety and soundness” in the context of protecting sensitive customer information and they have made no secret of this view.¹¹ The question remains, however, whether the Information Security Guidelines, as in effect in November 2004 when the alleged breach occurred, were sufficiently clear to put banks on notice that a particular method of disposing of records was "unsafe and unsound."

As to this question, the OCC would appear to have been on solid ground in its action against First Horizon: The Information Security Guidelines have specifically

¹¹ For example, in promulgating the Information Security Guidelines in final form in 2001, the agencies stated their belief that “a financial institution’s overall information security program is critical to the safety and soundness of the institution.” 66 FR 8616, 8620 (February 1, 2001).

referred to proper disposal of physical records containing sensitive information as a concern since they were first issued in final form in 2001. The preamble to that issuance noted:

The Agencies also have added a specific reference to records disposal in the definition of "customer information system." This is consistent with the proposal's inclusion of access controls in the list of items a financial institution is to consider when establishing security policies and procedures . . . *given that inadequate disposal of records may result in identity theft or other misuse of customer information. Under the final Guidelines, a financial institution's responsibility to safeguard customer information continues through the disposal process.*

66 Fed. Reg. 8616, 8618 (February 1, 2001) (emphasis added).

The importance of proper disposal of paper records, with a clear recommendation to shred paper records before disposal, was also emphasized in the Information Security Booklet (the "IS Booklet") released by the Federal Financial Institutions Examination Council in January 2003. In the subsection addressing Disposal of Electronic and Paper-Based Media, the IS Booklet stated:

Financial institutions need appropriate disposal procedures for both electronic and paper-based media. Policies should prohibit employees from discarding sensitive media along with regular garbage to avoid accidental disclosure. Many institutions shred paper-based media on site and others use collection and disposal services to ensure the media is rendered unreadable and unreconstructable before disposal. Institutions that contract with third parties should use care in selecting vendors to ensure adequate employee background checks, controls, and experience.

IS Booklet at 63.

The banking agencies' again noted their concern with proper disposal of sensitive records with the issuance of a *Request for Comment on Interagency Guidance on Response Programs to Protect Against Identity Theft* in August 2003. The proposed Interagency Guidance cited, as an example of when customers should be notified of

possible unauthorized access to sensitive information, when "[a]n institution has not properly disposed of customer records containing *sensitive customer information*." 68 Fed. Reg. 47954, 47960 (August 12, 2003) (italics in original).

Finally, in 2004, in the context of implementing Section 216 of the Fair and Accurate Credit Transactions Act of 2003 (the "FACT Act"), which requires proper disposal of *consumer* information derived from credit reports, the banking agencies reiterated the importance of proper disposal of *customer* information.¹² The Supplementary Information explaining the proposed FACT Act rule noted that proper disposal of sensitive customer information was *already* required under the Information Security Guidelines.

The Guidelines direct financial institutions to assess the risks to their customer information and customer information systems and, in turn, implement appropriate security measures to control those risks. For example, under the risk-assessment framework currently imposed by the Guidelines, each financial institution must evaluate whether the controls the institution has developed sufficiently protect its customer information from unauthorized access, misuse, or alteration when the institution disposes of the information.

69 FR 31913, 31914-31915 (June 8, 2004) (footnotes omitted).

Later in the same release, the agencies provided more specific information on their expectations regarding the proper disposal of sensitive customer information.

The Agencies believe that it is not necessary to propose a prescriptive rule describing proper methods of disposal. Nonetheless, consistent with interagency guidance previously issued through the Federal Financial Institutions Examination Council (FFIEC) [citing the IS Booklet excerpted above], the Agencies expect institutions to have appropriate disposal procedures for records maintained in paper-based or electronic form. *The Agencies note that an institution's information security program should ensure that paper records containing either customer or consumer*

¹² The distinction between "*consumer* information" for purposes of the FACT Act and "*customer* information" under the Information Security Guidelines is not relevant to the present discussion.

information should be rendered unreadable as indicated by the institution's risk assessment, such as by shredding or any other means.

69 FR 31913, 31916 (footnotes omitted; emphasis added)

In light of these agency pronouncements from January 2001 to June 2004, it seems fair to conclude that, by November 2004, banking organizations should have been on notice that they should not dispose of paper records containing sensitive customer information without shredding them or taking other protective measures. Considered against this backdrop, assuming that First Horizon was rightly found to have acted recklessly and to have met the other criteria for a second tier CMP, the OCC's action against First Horizon would not seem unreasonable.

Relying on the second tier CMP authority seems preferable from a policy perspective, as well, because it requires a greater degree of wrongful conduct before a penalty may be imposed. Safety and soundness is an inherently malleable concept, and the issuance of guidelines is an imperfect tool for informing the banking industry about what the concept requires in various contexts. There is a trade-off between flexibility and avoidance of overly prescriptive rules, on one hand, and the clarity and certainty that well-drafted rules and regulations provide, on the other. The potential for unfairness and undue harshness that exists when safety and soundness guidelines are enforced by civil money penalties is mitigated, if not entirely eliminated, by the requirement of recklessness and other prerequisites before a second tier CMP can be imposed. However fuzzy or imprecise may be the guidelines seeking to give content to the principle of “safety and soundness,” some conduct is so clearly reckless and improper that a civil money penalty can be justified. It does not seem defensible to

sanction a violation of "guidelines" based on the strict liability standard for first tier civil money penalties.

* * *

Peter Heyward welcomes comments and questions about this article. His e-mail address is peheyward@venable.com.