April 12, 2007

Information Collection Comments
Chief Counsel’s Office
Office of Thrift Supervision
1700 G Street, N.W.
Washington, D.C. 20552

RE:   Agency Information Collection Activities: Security Breach Notice Guidance

To Whom It May Concern:

The American Financial Services Association (“AFSA”\(^1\)) submits this comment letter in response to the OTS’s Notice and Request for Comment\(^2\) with respect to the interagency Security Breach Notice Guidance.\(^3\)

AFSA commends the federal banking agencies for their role in promoting security and confidence in the American banking system by establishing expectations for financial institutions with respect to information security standards, including response programs and customer notice requirements on the occasion of security breaches. Information security requirements for commercial enterprises – where most publicized security breaches have occurred – are established, if at all, by a patchwork of state laws. Despite various proposals, no federal law applies. For financial institutions, however, the standards are settled. Partly as a result, we believe consumer information in the possession of financial institutions is protected by security measures consistently higher than consumers enjoy with respect to most commercial enterprises. This is a good thing for the industry and for its millions of customers.

There is one subject-matter area to which we think the agencies could bring needed clarity, perhaps by publishing some FAQs associated with the Security Breach Notice Guidance. That area is the manner in which the Guidance applies to non-electronic customer information,

---

\(^1\) The American Financial Services Association, founded in 1916, is the trade association for a wide variety of consumer finance companies. AFSA’s mission is to protect and improve the consumer credit business, maintain a positive public image, and create a legislative climate in which reasonable credit regulation can and will be enacted. AFSA operates in the public interest, encourages and maintains ethical business practices, and supports financial education for consumers of all ages.


\(^3\) 70 Fed. Reg. 15736 (March 29, 2005).
and to various specific instances of regular occurrence to which the Guidance might or might not apply. Because the Guidance appears to have been drafted with computerized data in mind primarily, it does not unambiguously address the facts and circumstances of data security events that involve data that is reproduced or stored in other mediums. We believe that those events, in fact, represent the vast majority of all data security events (though generally not the most severe events). When a data security event occurs that involves non-computerized data, a financial institution intent upon fully complying with the letter and spirit of the Guidance is often left to guess as to exactly how and in what way the Guidance applies. This may in many cases result in conservative over-compliance, with unnecessary expense and customers receiving more notices than the agencies would believe necessary and appropriate. Conversely there may be cases in which an institution interprets the Guidance as not covering an event when the agencies would believe that it does, so that customers do not necessarily receive consistent notices with respect to the same events at different institutions.

For these reasons, AFSA requests that the OTS, in consultation with the other agencies, publish FAQs regarding the Guidance that clarify the agencies’ views of how the Guidance applies to various fact patterns that can arise with respect to non-computerized customer information. Although we believe the agencies should perform some form of outreach to industry to solicit topics and areas to be addressed by any such FAQ guidance, such as by publishing a request for comments specifically directed to issues around non-computerized customer information, we believe that the following situations and issues arise with sufficient frequency that they should be addressed:

- Should mail systems operated by the United States Postal Service or private carriers be considered a part of a financial institution’s customer information systems for purposes of the Guidance? The Guidance states that every financial institution should “require its service providers by contract to implement appropriate measures designed to protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.” In the case of the Postal Service, it may be difficult for financial institutions to require procedures different from those that the Service applies to all mailers.
- Has a breach subject to the Guidance occurred if an item containing sensitive customer information is inadvertently sent to the wrong address and is opened? We suggest not, because the information is out of the institution’s customer information system at the time the unauthorized access takes place.
- Has a breach subject to the Guidance occurred if a financial institution uses skip tracing to identify an alternative address for a customer that it cannot otherwise reach and the letter is opened by a non-customer at that address? We suggest not, because again, the information is out of the institution’s customer information system at the time the unauthorized access takes place.
- Suppose a document containing sensitive customer information is lost in transmission by a mail carrier. Is this incident subject to notice requirements under the Guidance? We suggest not, because there has been no confirmed instance of unauthorized access to customer information.

---

• Should a breach for purposes of the Guidance be deemed to have occurred if a document containing sensitive customer information is faxed to what is later determined to be a wrong number and a fax confirmation is generated by the sending fax machine? Because working fax machines are rarely unattended, this could be regarded as a breach for purposes of the Guidance.

• Suppose a non-customer who inadvertently receives a customer’s sensitive customer information notifies the financial institution of the event. Should this require notice under the Guidance? What if the non-customer indicates that he or she destroyed the information, or returns the information to the financial institution? We submit that in these cases it is not “reasonably possible,” under the Guidance, for misuse of the information to occur, because a person would not plausibly report the incident to the transmitting financial institution and then attempt to use the customer information to commit fraud.

• May a financial institution delay customer notice under the Guidance in order to investigate the size of the pool of customers affected by a data security incident? The Guidance implies that this is appropriate in its discussion of affected customers.

• Sometimes the number of “affected customers” within the meaning of the Guidance is very small but it is not known who they are out of a much larger population. For instance, what if a service provider informed its financial institution that 10 of the 1 million accounts for which it maintains account transaction data were compromised, but the service provider had no way of knowing exactly which 10 accounts? Or, what if a vendor hired to destroy 1 million documents containing account information for 1 million different accounts informed its financial institution that it received and destroyed only 999,990 documents, and neither the vendor nor the financial institution had the ability to tell which documents had been lost instead of destroyed? Does the Guidance require that in each of these cases 1 million customer notices must be sent? If the agencies believe that the Guidance establishes a risk-based regime and should not be read to require this degree of vast over-noticing, with unnecessary fear and alarm among many consumers, an FAQ could be an appropriate means to express that interpretation.

All of these situations, and possibly many others that an inquiry to the industry could reveal, could appropriately be resolved by publication of informal interpretations of the guidance, such as by FAQs.

We appreciate the opportunity to respond to the Notice. If you have any questions about this letter, please contact the undersigned at (202) 466-8606.

Sincerely,

Robert McKew
Senior Vice President and General Counsel
American Financial Services Association