

ROBERT H. CARPENTER, JR.

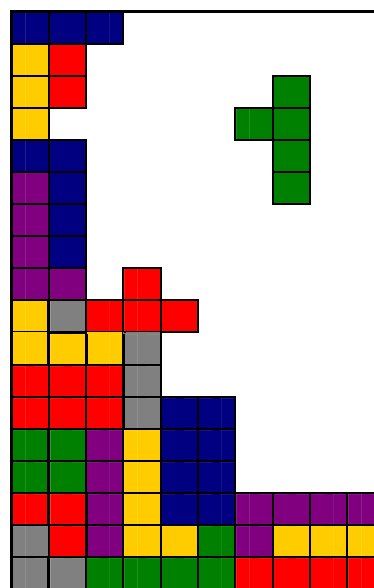
ATTORNEY AT LAW
5912 CASTLEBAR LANE
PLANO, TEXAS 75093

TELEPHONE 972.473.4834

email: Bob.Carpenter@CarpenterLaw.net

www.CarpenterLaw.net

September – October 2008



*"The Perfect Fit for
Your Business"™*

 **WARNING**
... the **FACT(A)** is ...

November 1 is the deadline; and 84% of bankers may not have done anything, or enough, to be ready.¹ And, those companies that provide outsourced information technology services to financial institutions are not likely to be ahead of their customers. What is this FACT(A), and how might it affect outsourced services?

The identity theft provisions of the Fair and Accurate Credit Transactions Act of 2003, or FACT(A), are summarized in the rulemaking:

Section 114 of the FACT Act requires the [Federal banking agencies and the FTC] to jointly issue guidelines for financial institutions and creditors regarding identity theft with respect to their account holders and customers. Section 114 also directs the[se] Agencies to prescribe joint regulations requiring each financial institution and creditor to establish reasonable policies and procedures for implementing the guidelines, to identify possible risks to account holders or customers or to the safety and soundness of the institution or "customer."

In developing the guidelines, the[se] Agencies must identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft. . . . These guidelines would provide that in such circumstances, a financial institution or creditor "shall follow reasonable policies and procedures" for notifying the consumer, "in a manner reasonably designed to reduce the likelihood of identity theft."²

This mandate seems pretty straightforward, but is likely to be time-consuming to implement. That is probably why so many financial institutions are behind in their plans. Remember, the FACT(A) was enacted in 2003 and the final implementing rules were adopted in late 2007; so there has been plenty of warning.

¹ Tripp Johnson, *Wave That Flag – But You Best Hurry*, GONZOBANKER, Sep. 5, 2008, <http://gonzobanker.com/article.aspx?Article=394>.

² Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63,718, 63,719 (Nov. 9, 2007) (to be codified at 12 C.F.R. pt. 41 (OCC), 12 C.F.R. pt. 222 (FRS), 12 C.F.R. pts. 334 and 364 (FDIC), 12 C.F.R. pt. 571 (OTS), 12 C.F.R. pt. 717 (NCUA), and 16 C.F.R. pt. 681 (FTC)) (footnotes omitted) [hereinafter FACT(A) Rule].

What seems less obvious is how all of this, or any of this, applies to companies to whom financial institutions have outsourced information technology services. What is clear – there is application to those service providers because the final rule, although mentioning outsourced services in only a few places, provides this:

Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider’s activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.³

Of course, financial institutions are primarily responsible for implementation of the “Red Flag Rules” and for oversight of their service providers when those service providers engage in activities that could give rise to identity theft. In exercising this newest vendor management responsibility, financial institutions should carefully evaluate their outsourced activities; not all of them will present identity theft risk.

The outsourced activities that present the most obvious identity theft risk are those in which the service provider receives and processes identity information directly from the customer, rather than receiving it from the financial institution. In such cases, the service provider should include in its offering the functionality “to detect, prevent, and mitigate the risk of identity theft.”

Several services in that high-risk category include Internet banking, including Internet account establishment, and remote deposit capture. And, how about Fiserv’s new MyMoney™ built on the Facebook® Platform or the Fiserv Mobile Money™ solution? As services expand their reach via new and innovative means like these Fiserv offerings, identity theft challenges will increase, maybe exponentially because the growth in such new product delivery channels is predicted to be exponential.

If bankers have not prepared for November 1, maybe their service providers have not either. Evaluating outsourced technology services for identity theft prevention tools is part of a financial institution’s overall vendor management program responsibility as well as the specific charge of the new “Red Flag Rules.”

© 2008 Robert H. Carpenter, Jr.

This client newsletter is for informational purposes only, and is not intended to be legal advice. Transmission of this newsletter is not intended to create, and its receipt does not establish, an attorney-client relationship. Legal advice of any nature should be sought from legal counsel.

TREASURY DEPARTMENT CIRCULAR 230 DISCLOSURE: Any Federal tax advice set forth in this communication is not intended or written to be used, and cannot be used, for the purpose of (1) avoiding penalties that may be imposed by Federal tax laws or (2) promoting, marketing or recommending to another person any transaction or matter addressed herein.

³ FACT(A) Rule at 63,755.

FTC Delays FACT(A) Enforcement

Despite the advance warning, the FTC announced on October 22, 2008 that it would delay enforcement of the “Red Flags Rule” until May 1, 2009. The FTC, in issuing its enforcement policy, said, “. . . some industries and entities within the FTC’s jurisdiction have expressed confusion and uncertainty about their coverage under the rule. These entities indicated that they were not aware that they were undertaking activities that would cause them to fall within FACTA’s definitions of “creditor” or “financial institution.”

To date, the Federal banking agencies, including the NCUA, have not issued any enforcement delays for the identity theft “Red Flags Rule” for financial institutions within their jurisdictions.