

## RDC compliance remains thin

Few banks realize the broad scope of FFIEC guidance

By Dan Fisher, president and CEO, The Copper River Group, Fargo, N.D., and a regular blogger on ababj.com ("Beyond the Bank"). His firm focuses on technology and payment systems research and consulting for community banks. dan@copperwombat.com

Few banks are aware of the broad scope of FFIEC guidance on the risk management of remote deposit capture

In January of this year, the FFIEC issued the long awaited guidance on remote deposit capture. The industry expected the guidance to address the use of check scanners by commercial customers. The guidance, however, is much more far reaching and carries with it a significant impact on the management of technology. The comprehensive nature of the FFIEC definition of RDC means that any place where deposit documents are scanned—ATMs, branch (back counter), commercial (merchant), consumer (retail), kiosk, or back office—and any device for doing so including cell phones, faxes, and emails (with scanned checks attached) are covered by the guidance, not just merchant capture.

Furthermore, the FFIEC clarified the definition of remote deposit capture technology as a transaction delivery system that results in the movement of money. So, institutions need to be mindful of the additional regulatory implications in regard to the Bank Secrecy Act, Gramm-Leach-Bliley, and the Patriot Act.

### Early exam findings

Shortly after the release of the guidance, Tony DaSilva, a bank examiner with the 6th Federal Reserve Bank of Atlanta, gave a presentation summarizing the RDC exam findings in the 6th Federal Reserve District in regard to the FFIEC guidance and compliance. The top five findings were:

- Lack of senior management oversight;
- Lack of adequate MIS and reporting
- Lack of monitoring;
- Inappropriate approval process (separation of duties);
- Inadequate limits or no limits.

With the newness of the guidance and the preoccupation of the industry with the financial crisis, it would be an understatement to say that bank management was focused on other things. The findings are, nonetheless, the findings. Questions need to be asked, especially: Has progress been made in the 11 months since the release of the guidance?

### Understanding limited

Many bank executives do not yet understand the broad scope of the FFIEC definition of RDC, according to Patti Murphy, president of the Takoma Group and an expert on check technology. But, she adds, "the guidance is bringing to

the forefront the issue of risk management and the fact that compliance will not gain traction without senior management attention." Susan Orr, of Susan Orr Consulting, agrees, and says that, "understanding IT risk is not a priority right now when the industry is focusing on other issues such as credit quality."

Dan Haffner, director of SAS and Item Processing Services at Myriad Systems, Oklahoma City, comments that, "most FIs do not understand, but quickly become hyper focused after examiners start asking questions about RDC compliance."

Barry Landry, senior vice-president of C&A Associates, Denham Springs, La., (an RDC vendor) adds that the majority of banks have not had an RDC exam.

C & A Associates and Myriad Systems are both developing system application changes that will aid their clients with compliance, particularly in the area of activity monitoring, a central theme of the guidance.

RDC increases risk, but how much?

The thrust of the guidance points directly to the increased risk associated with the implementation of remote deposit capture and the need for banks to take deliberate measures to identify, assess, manage, monitor, and mitigate this risk. The guidance is very clear in the expectations of the role of management, and about how the increased technology risk is managed.

Clifton Stanford, director of the Atlanta Fed's Retail Payments Risk Forum, says that RDC raises a range of issues regarding financial services products, including the emerging role of independent sales organizations (ISOs) into the mix, remotely created checks, and consumer capture. Sanford reminds institutions that they "need to be thorough in their due diligence, being sure to identify the associated risks," in advance of implementing any new RDC technology or product.

Barry Landry of C&A Associates mentions that even though remote capture has grown significantly since the enactment of Check-21—particularly with commercial customers—the penetration rate is very low and thus the increased risk may be hard to quantify. Paul Carrubba, a legal expert on payment system law with Adams and Reese, conveys that, "most financial institutions are being diligent on the front end and have limited the offering of RDC to only their best customers. Thus the risk, by virtue of an existing and strong relationship, is going to be low." Carrubba cautions that the low risk and lack of identified RDC losses, at this juncture, could easily lull a bank into a false sense of confidence and subject it to an unknown, or at least an unexpected, risk particularly if it does not continuously monitor ongoing RDC activity.

Little monitoring going on

The guidance outlines that financial institutions are to monitor their RDC activity, but there is confusion about what institutions are to monitor and how it is to be reported. One of the mission-critical aspects of the guidance, however, is not only to monitor RDC activity, but also to have the ability to take action in the event that an operating threshold is exceeded, be it at a branch or at a customer location. It should also be pointed out that the exam findings cited earlier identified the lack of adequate MIS reporting and lack of monitoring as being number two and three on the top-five list. The translation is simple one: looking at a threshold-limit violation 30 days after the fact is not an effective risk management, monitoring, and mitigation program.

An example of an inadequate MIS finding would be bank installing an RDC application that only scans checks and is incapable of monitoring RDC activity intra-day; or not stopping a transaction until after the scanned item has posted to the institution's DDA system and the electronic cash letter is already out the door (post-facto intervention). Lack of reporting refers to not having an established process of reporting incidents to senior management or the board of directors. Reportable incidents can include trends in RDC related losses, customer limit violations, or compliance violations of organization's RDC risk management policy.

In both of these cases, an organization's ability to respond to a deteriorating situation, once senior management becomes aware of the problem, would be reactive in nature, which is contrary to the guidance that focuses on identifying, assessing, managing, monitoring, and mitigating RDC risks up front. The theory of the guidance is to look ahead to see a potential problem rather than look back and realize you have one.

Has RDC increased fraud losses?

Susan Orr, observes that the losses that are occurring are most likely not being attributed to RDC or not reported at all. Paul Carrubba clarifies that if losses occur, they will not come from an institution's best customers. He cautions, however, that even your best customers should be continually monitored for any significant changes in the deposit activity or relationship deterioration.

It should be pointed out that all of the individuals interviewed for this article agree that the level of losses that can be attributed to any form of remote deposit capture are unknown. As banks expand their offering to include more businesses, and specifically consumer customers, the risk of losses and abuses will increase. Banks need to remain vigilant in monitoring changing risk characteristics.

Fed research needed

As a part of the Check 21 legislation, the Federal Reserve is required to report to Congress on a regular basis the law's effects on the check clearing system. In providing that data, the Fed has not to date included a survey of any negative impacts of Check 21 and increased fraud losses. Clearly if the industry is going show improvement, there should be a benchmark. It stands to reason, as the number of RDC implementations go up, so will fraud losses.

A similar situation existed for years with check fraud until a survey was completed by the ABA, which found that banking industry check fraud losses exceeded \$900 million annually (in the 1990s). The quantified losses indeed caught the industry by surprise.

The same may be true about RDC losses. But at the present time, such losses are not reported and no comprehensive survey of losses has been conducted as more RDC technology is being deployed in and outside of banks.

What banks need to do

Timing being everything, industry awareness is the key to complying with the FFIEC guidance on the risk management of remote deposit. The five exam findings cited earlier should serve as a checklist for banks to use as they begin to develop and implement an RDC compliance program.

Banks do respond quickly when they are made aware of the guidance. Compliance, however, should not be a post-facto event. Monitoring internal RDC activity and identifying losses, then preventing re-occurrence is central to the guidance; however, it would be helpful to the industry if the Federal Reserve System could serve as the information clearinghouse on RDC related fraud scenarios, losses, and trends.

More work needs to be done to create an industry-wide appreciation of the technology risks associated with remote deposit capture and that includes management at the highest levels of the organization. In this case, compliance should be a top- down event. BJ

The electronic version of this article available at: <http://www.nxtbook.com/nxtbooks/sb/ababj1209/index.php?startid=28>