

## Remote Deposit Capture: Who's Minding the Store?

It has been over three years since The Check Clearing for the 21st Century Act, aka Check 21, was passed. Financial institutions can now attract commercial customers and streamline costs using technology that allows checks to be processed more efficiently. This service—Remote Deposit Capture or RDC—has been touted as a competitive advantage by financial institutions looking to differentiate themselves in the marketplace. Gone are the days when your local merchant had to leave his store to make the deposit deadline. Now, he can just scan paper checks and electronically send business deposits to his bank with the touch of a button, all without leaving his own place of business.

Perhaps your bank has been contemplating using RDC as a marketing strategy to attract and retain customers or maybe your bank has just started offering this service. As with any new service, there are risks and benefits which will ultimately affect a bank's business decision. The obvious benefits of RDC are more convenience for the merchant, along with reduced costs for both the merchant and the bank. However, this service creates its own set of risks, as RDC essentially causes the bank to place some of its check operations into its customers' hands. This increases the potential for electronic checks to be altered or counterfeited by criminals who may be more computer-savvy than the client. RDC also creates the possibility that the physical checks, which are now kept at the merchant's store, may be stolen, altered, and deposited at another branch or bank.

Here are issues that your bank should consider to minimize the risk associated with offering RDC:

### **Know your customer and be selective**

It is prudent for any bank to know its customers before offering this service because the client is now acting as a check collector/processor, whereas prior to RDC, merchants solely acted in a client capacity. To conduct effective due diligence, understand the type of business in which your commercial customer is engaged. For example, it won't make sense to offer RDC to a business that has a high frequency of fraudulent activity among its employees. Assess the physical security of the merchant's place of business. Is it easy for customers to access the areas where the employees work? These types of questions must be asked before the bank agrees to offer RDC services to its customers. To address these issues, the bank should require a completed application from potential RDC customers to properly evaluate each customer on an individual basis. Remember, it is just as important to review and assess RDC clients as you would with an ACH or even a loan client. A good candidate for RDC would be a trusted, long-time customer, with a favorable account history, who has the capability and expertise to understand the technology and the risks associated with RDC.

### **Educate your customer and set clear guidelines**

Since RDC involves check processing and technology, it is important to have a good understanding of these issues, from

both a bank and merchant/client perspective. While the banker may already understand how this technology works, it is unlikely that the merchant will have as good an understanding because he or she may not be used to the compliance issues that banks face, and therefore, may not understand the security risks associated with RDC. Customers should be informed about the importance of dual controls and segregation of duties, which are essential to limiting the potential for RDC fraud. Before signing up customers for RDC, draft specific agreements that contain clear and logical guidelines. The agreements should carefully spell out both parties' responsibilities and the bank's expectations of its customers, such as the agreed-upon check retention and destruction policies, safeguarding of checks, etc. If the bank does not provide the scanners, then the agreement should specify the type of scanner required. A high-quality scanner is critical to deter fraudulent check activity. Poorly scanned checks are an easy target for criminals. Additionally, to limit future disputes, the liability of both parties should be addressed in the agreement. Lastly, the agreement should allow your bank to periodically audit its customers to ensure that these clients are abiding by the terms of the agreement.

### **Carefully choose a vendor**

It is smart to use a reputable vendor, perhaps one that your bank already knows and trusts. The most obvious area to review when choosing a vendor is security. It is absolutely critical that the vendor provide a secure mechanism that will protect the bank from fraudsters. Banks also need to carefully review contracts to make sure that the liability of both parties and "hold harmless" agreements are fair to the bank. Most, if not all, vendors provide added features such as duplicate check detection or other fraud detection software, so make sure that you are getting the most from your vendor; **make sure that this agreement is written into the contract to avoid potential problems if a loss occurs.** There have been cases in other operational areas, like credit card processing, where banks thought they had enhancements, but the contract stated otherwise. The bottom line is that the bank must be careful to assess each potential vendor in order to protect itself from losses.