

SafeAlert



A loss control advisory from the ABA-sponsored insurance program underwritten by Progressive

Remote Deposit: Minimize Your Exposure to Fraud

Bankers focusing on issues surrounding image and transmission quality of Remote Deposit technology need also be conscious of potential fraud exposures.

Deflecting liability does not minimize the risk to your reputation when a perpetrator takes advantage of easy access through technology.

Many bankers rely on hold harmless agreements to put liability for fraud in the customer's hands; however, deflecting liability does not minimize the risk to your reputation when a perpetrator takes advantage of easy access through technology. More importantly, if the customer itself is the perpetrator - or even if not - funds may not be available to reimburse the bank.

Focus increased attention to these basic bank practices to minimize exposure:

- ☑ If Remote Deposit is a tool for pursuing new customers outside the bank's footprint, "Know Your Customer" becomes more important than ever. Screen businesses to make sure that they have a reputable track record; visit the business and evaluate the deposit customer as a credit risk, just as you would for a potential ACH or ARC customer.
- ☑ Audit the customer's business processes that surround the remote deposit process: is the customer technically and functionally mature enough to handle check processing and control? The customer should be able to exhibit segregation of duties and controlled access of these negotiable instruments - before, during and after scanning.
- ☑ Understand how the customer intends to store the checks, how long they will be kept, and how they will be disposed of (shredder or dumpster?). Investigate who has building access, and who has access to both the documents and the images from the customer side. Make recommendations on segregation, access and disposal processes and follow up to ensure they are followed.
- ☑ Evaluate the customer's IT security - the firewalls and security in which you have so heavily invested are equally important on your customer's systems if check images reside on them.
- ☑ Explore the Remote Deposit vendor's fraud mitigation technology. Do not assume that fraud detection software is in place unless specified in the contract.
- ☑ Make sure that all the bank's associated exception processes - signature verification, large item review, stop payment - are appropriately integrated for Remote Deposit accounts.
- ☑ Focus increased attention to exception reports on Remote Deposit accounts to understand business volumes and detect any unusual activity.

For more information, contact Judi Kovach, Loss Control Manager at 800-274-5222.