Two Ways to Mitigate Remote Deposit Capture Risk

The success that banks have had deploying remote deposit capture has been tremendous over the past few years. The ability to decrease manual handling of checks and increases deposit breadth has certainly been a positive in what otherwise has not been the greatest of times in the banking community. However, as with any success along comes scrutiny. Echoes from the halls of Congress of not enough transparency, FFIEC urging tighter controls and risk mitigation of "remote capture", not to mention pay caps or increased FDIC premiums; has taken much of the wind out of the sails of banks innovation in the past year.

Much has been written of the risks associated with RDC, many influential people and companies have weighed in on the steps that can be taken to mitigate the risk of fraud and abuse, but few to none have actually developed solution(s) that truly mitigate the risks that the FFIEC has issued guidance on. Creating processes, control points, verification steps or reports as a way to handle them are all just band aids to cover the glaring problems. A solution that is designed to address these issues head on is what the industry needs to quiet the masses of nay sayers, offer clients superior service and continue to compete in a fast paced demanding market which is constantly evolving.

ImageScan Inc., a leading provider of transactional content and processing solutions, long known for their ability to meet the complex needs of the financial service industry has two such solutions. The first, *Remote Transaction Capture*, which can be deployed as a module within a back office department offers fully integrated workflow of remotely captured checks and also has the added benefit of being capable of scanning full page or remittance items. The second, *TCM Unify®* provides the ability to acquire, aggregate, normalize and manage content from disparate systems like typical stand alone Remote Deposit Capture products, enabling a bank to perform sub-process or verification steps and full archive capabilities for these items. These two different approaches offer varying mitigation levels of risk, based on a banks appetite and risk tolerance.

The chart below describes in detail how each solution enables banks to mitigate risk, provide superior customer experiences, while continuing the deep penetration that traditional Remote Deposit Capture products enjoy.

For additional information, please contact ImageScan at 301-306-0700.

FFIEC Statements - Issued 1/2009 "Risk Management of Remote Deposit Capture"		**Remote Transaction Capture**	**RDC Integration via TCM Unify®**
Legal & Compliance Risk			
	"The institution should consider whether and to what extent it could be exposed to the risk of money laundering activities as well as its ability to comply with anti-money laundering laws and regulations and suspicious activity monitoring"	Mitigating money laundering risk is an essential piece of the Remote Transaction Capture product. One of the key aspects is the separation of tasks, requiring bank personnel or bank controlled technology to perform balancing of remote captured items. This separation of tasks puts the final disposition of the remote captured item in the banks control, not the individual client doing the scanning of items, unlike typical RDC products.	Integration of Remote Deposit Captured items into a banks operating unit workflow, can mitigate the risks associated to money laundering activity. For instance a lockbox department, validates the negotiability of every item processed and is well versed in AML processes and procedures, and routinely performs OFAC checks. TCM Unify can present all or a subset (spot check) of items for review to qualified financial institution associates.
Operational Risk			
	"Faulty equipment, inadequate procedures, or inadequate training of customers and their employees can lead to inappropriate document processing, poor image quality, and inaccurate electronic data."	Remote Transaction Capture, in of itself is a capture only process - enabling the bank to control which items are accepted, perform IQA, make correction where necessary or completely reject an entire batch if necessary. All of these options and tasks are performed by bank personnel or agents on their behalf, in controlled environments with all the proper processes and procedures in place, including employee training, IQA knowledge and zero defect goals.	Utilizing an RDC system as the capture process only, would enable the bank to perform all of its rigorous IQA it would on a physically presented items. With the IQA performed and controlled at the bank, much of the downstream risk for client error is negated.
	"Ineffective controls at the customer location may lead to the intentional or unintentional alteration of deposit item information, resubmission of an electronic file, or re-deposit of physical items."	Remote Transaction Capture offers two levels of duplicate detection to mitigate the unintentional processing of physical items; at the remote location duplicate detection is deployed and stored for 30 days while at the central location duplicate detection can be configured to meet the banks risk strategy. This in addition to the separation of the capture, balance and deposit tasks, enables full control of "acceptance" criteria to be the banks alone.	Standalone RDC products do not offer the opportunity to deploy duplicate detection outside of the silo in which they are processed. As a result of integrating all payments streams via TCM Unify, duplicate detection can be deployed and suspects identified regardless of how the items are presented.
	"Inadequate separation of duties at a customer location can afford an individual end-to-end access to the RDC process and the ability to alter logical and physical information without detection."	One of the main benefits of the Remote Transaction Capture module is the ability to separate tasks, to complete a deposit. Essentially your clients' remote location becomes a capture only process, integrating the captured checks and associated documents into the central workflow for negotiability scan, balancing, value added processing such as float reporting, data entry or scanline repair, and finally deposit creation. This separation of tasks is a critical component to mitigating alterations and potential fraud that first and second generation Remote Deposit Capture products lack.	TCM Unify can enable the detection of duplicate payments regardless of the method of payment. Integrating your banks RDC items, would allow for a duplicate detection check, same day as the processing occurs allowing for the bank to place holds on suspicious items or reject duplicate items.

	"technology-related operational risks include failure to maintain compatible and integrated IT systems between the financial institution, service providers, and the customer "	The Remote Transaction Capture module has a smart client design, to ensure that upon log-on by the remote customer; a logical check is performed ensuring that both the financial institution and the remote location are compatible. If this check fails, the central location will push the appropriate update files to the remote location before any images can be submitted.	
	"Check alteration, including making unwarranted changes to the Magnetic Ink Character Recognition (MICR) line on the image of scanned items, may be more difficult to detect when deposited items are received through RDC and are not inspected by a qualified person."	The act of inspecting items is a core competency for the processing of wholesale or retail lockbox items; as such the employees in this department(s) are well trained in the negotiability of an item. In addition, business rule and criteria verifications like OFAC compliance or individual client acceptance criteria is part of every item received by these departments standard practice. There is no other operating unit, with the exception of a branch teller, that is uniquely qualified to handle such items, than a lockbox department.	Utilizing an RDC system as the capture process only, would enable the bank to perform all of its rigorous IQA it would on a physically presented items. With the IQA performed and controlled at the bank, much of the downstream risk for client error is negated.
	"The potential for insider fraud may be greater with RDC because the financial institution typically does not perform background checks on its customers' employees who may have access to physical deposit items or electronic files."	The integration of this remote product would mostly likely occur in a lockbox department, an established Treasury Management Agreement would be recommended further mitigating liability of the bank from said clients' employee fraud. In any such agreement the customer would typically warrant things such as: all IQA standards would be met, only acceptable items would be deposited, processes to control duplicate files or items would be in place, customer would not deposit the physical item, all information is accurate and free of false claims, customer has complied with all rules, regulations and/or statutes, and customer indemnifies the bank from any loss for breach of warranties. Not only would the language of a TMA be reflective of the protections and processes, but most banks undergo account reviews on a periodic basis that would further mitigate risk by exposing, changes to locations, facilities, and/or financial activity.	
Customer Due Diligence and Suitability			
	"In general, information gathered while conducting customer identification and customer due diligence procedures in fulfillment of the institution's BSA/AML program can support the assessment of customer suitability."	Lockbox is considered a Treasury Management product at most financial institutions; a standard practice of opening any new TM relationship would fulfill these requirements and in most cases exceed these requirements.	
	"For new and existing customers, a suitability review should involve consideration of the customer's business activities and risk management processes, geographic location, and customer base."	Lockbox is considered a Treasury Management product at most financial institutions; a standard practice of opening any new TM relationship would fulfill these requirements and in most cases exceed these requirements.	

Vendor Due Diligence and Suitability			
	"Financial institutions' interest in RDC has led to a proliferation of RDC technology service providers and RDC hardware and software suppliers. Financial institutions that rely on service providers for RDC activities should ensure implementation of sound vendor management processes as described in the Outsourcing Technology Services Booklet of the FFIEC IT Examination Handbook."	ImageScan has a long relationship in the financial services community, providing leading edge software processing capabilities since the early 1990's. As a strong partner, ImageScan operates under many vendor management programs, reporting requirements and auditing analysis from some of the nation's largest financial institutions. In addition to servicing banks, thrifts and insurance companies, ImageScan has a strong client base amongst state governments, adhering to many different levels of vendor management practices.	ImageScan has a long relationship in the financial services community, providing leading edge software processing capabilities since the early 1990's. As a strong partner, ImageScan operates under many vendor management programs, reporting requirements and auditing analysis from some of the nation's largest financial institutions. In addition to servicing banks, thrifts and insurance companies, ImageScan has a strong client base amongst state governments, adhering to many different levels of vendor management practices.
RDC Training for Customers			
	"Without effective periodic training, RDC customers may have unrealistic expectations of the system or may not understand their roles in managing risks and monitoring for processing errors or unauthorized activity. Management should ensure that customers receive sufficient training, whether the customer obtains the RDC system from the financial institution or from a third-party servicer. Sound training should include documentation that addresses routine operations and procedures, including those related to the risk of duplicate presentment and problem resolution."	All ImageScan products have E-Learning modules that can easily be made accessible to a financial institutions end clients. In addition, the use of a "smart client" enables the financial institution to "push" information to any or every client on an ad-hoc basis, upon the clients' login. This utility can be used to update clients on issues, trends, security awareness, and change to bank procedures or simply as refreshers or reminders.	
Contracts and Agreements			
	"Strong, well-constructed contracts and customer agreements are critical in mitigating the financial institution's risks."	The integration of this remote product would mostly likely occur in a lockbox department, an established Treasury Management Agreement would be recommended further mitigating liability of the bank from said clients' employee fraud. In any such agreement the customer would typically warrant things such as: all IQA standards would be met, only acceptable items would be deposited, processes to control duplicate files or items would be in place, customer would not deposit the physical item, all information is accurate and free of false claims, customer has complied with all rules, regulations and/or statutes, and customer indemnifies the bank from any loss for breach of warranties. Not only would the language of a TMA be reflective of the protections and processes, but most banks undergo account reviews on a periodic basis that would further mitigate risk by exposing, changes to locations, facilities, and/or financial activity.	The integration of this remote product would mostly likely occur in a lockbox department, an established Treasury Management Agreement would be recommended further mitigating liability of the bank from said clients' employee fraud. In any such agreement the customer would typically warrant things such as: all IQA standards would be met, only acceptable items would be deposited, processes to control duplicate files or items would be in place, customer would not deposit the physical item, all information is accurate and free of false claims, customer has complied with all rules, regulations and/or statutes, and customer indemnifies the bank

			from any loss for breach of warranties. Not only would the language of a TMA be reflective of the protections and processes, but most banks undergo account reviews on a periodic basis that would further mitigate risk by exposing, changes to locations, facilities, and/or financial activity.
Business Continuity			
	"The financial institution's business continuity plan should address RDC systems and business processes, and the testing activities should assess whether restoration of systems and processes meets recovery objectives and time frames."	Most financial institutions have very robust business continuity plans for the lockbox departments, the very nature of the clients served in these departments expect it. As such, remote lockbox would be covered within this BCP plan, accounting for the different severity levels of resumption the depositing bank deems necessary to restore service.	
Other Mitigation and Controls Considerations			
	"Separation of duties or other compensating controls at both the institution and the customer location can mitigate the risk of one person having responsibility for end-to-end RDC processing."	Remote lockbox integration to a central environment enables the separation of the capturing of items from the deposit creation tasks, with the final disposition of the items acceptability and negotiable amount squarely in control of the financial institution. In addition roles based security can be deployed at the financial institution to further separate tasks associated with RDC deposits, such as MICR correction or Check 21 processing.	TCM Unify can enable the detection of duplicate payments regardless of the method of payment. Integrating your banks RDC items, would allow for a duplicate detection check, same day as the processing occurs allowing for the bank to place holds on suspicious items or reject duplicate items.
	"Strong change control processes coordinated between the institution and customer can help to ensure synchronized RDC platforms, operating systems and applications, and business processes."	The Remote Transaction Capture module has a smart client design, to ensure that upon log-on by the remote customer; a logical check is performed ensuring that both the financial institution and the remote location are compatible. If this check fails, the central location will push the appropriate update files to the remote location before any images can be submitted.	Utilizing an RDC system as the capture process only, would enable the bank to perform all of its rigorous IQA it would on a physically presented items. With the IQA performed and controlled at the bank, much of the downstream risk for client error is negated.
	"To reduce the risk of items being processed more than once, deposit items can be endorsed, franked, or otherwise noted as already processed."	Physical endorsement or "franking" is available with Remote Transaction Capture, however it is dependent on the hardware device the item is captured. All images have virtual endorsement capabilities.	Virtual endorsement is available for RDC items that are cleared through the TCM Unify Check 21 module.