Meeting FFIEC Guidelines with the Right Check Scanner

DIGITAL CHECK | THE SECURE CHOICE™

How The Right Check Scanner Can Help Financial Institutions Meet Remote Deposit Capture Guidelines

Addressing issues raised in FFIEC's Risk Management of Remote Deposit Capture

As financial institutions find themselves facing additional risks related to the remote deposit capture process, they need to consider all avenues available to lower or limit those risks. Included in this risk assessment is selecting the check scanner with the appropriate technologies.

Digital Check provides banks, credit unions and their business customer's full-featured check scanners for remote deposit capture services that include all of the attributes expressed in the Federal Financial Institutions Examination Council's *Risk Management of Remote Deposit Capture* guidelines. These scanners are also priced to meet the modest budgets of most small businesses.

Below is a review of the guidelines and a high-level overview of how Digital Check's CheXpress® CX30 Scanner helps financial institution customers address these issues.

Each financial institution should make an overall assessment of its environment, policies, procedures and IT infrastructure in order to provide adequate protection of sensitive customer information. The report summarizes this as the following: "As an institution implements RDC systems, it must consider information security risks associated with RDC technology and operations" (Federal Financial Institutions Examination Council [FFIEC], 2009, p. 2).

Creating a secure RDC process depends on the soundness of a financial institution's customers using RDC as well as on its hardware and software partners.

Customer-Related Risks

The guidelines address the inherent risk associated with customer usage with the following: "Implementing RDC in the institution's backroom operations may present less risk and complexity than deploying RDC at remote locations, such as customers' business premises or homes, where the capture process is outside the direct control of the institution. Risks may differ if the institution uses image exchange for a portion of the process or elects to use the ACH network throughout" (FFIEC, 2009).

Each institution should assess how and where it deploys RDC and assesses and adjusts for the risks with each type of implementation.

The ability to create audit trails to mitigate the potential risk of fraud is of utmost importance. Digital Check's application programming interface (API) enables software companies, and banks to tightly control information captured at each scanner. Not only can scanners be associated to a specific RDC customer via the unique scanner serial number, but the check image can also be associated to the scanner via the serial number embedded in the image record. The image can also be identified as original via CRC16 or cyclic redundancy check of the image file. This process indicates whether any data has changed with the image file received versus the file sent. If the image data has been modified after capture, the CRC16 check result will not match and the item can be flagged for further review. A bank can further

tighten it's control of the RDC process by associating the customers PC to scanner via its internet MAC address.
The report also recommends that "senior management should identify and assess exposure to legal and compliance risks related to RDC" (FFIEC, 2009). It illustrates the following example of the correlation between established controls and check settlement: "If a financial institution accepts a deposit of check images from a customer through the RDC system, legal risk exposures may be related to the controls over the process used for image capture or image exchange and the institution's arrangements and contracts for clearing and settling checks" (FFIEC, 2009).

In other words, the more controls management can establish in the process, including actions such as a physical endorsement *and* the use of a franking mark, the lower the risk of potential fraud or mistakes.

Training for financial institutions' employees and small business customers is essential to mitigating RDC risk. The easy-to-use design of the CheXpress© CX30 requires no customer assembly and has a one-piece cover that keeps out foreign objects. With only one way to insert checks, the scanner is intuitive to use. Digital Check offers training materials and videos, along with access to a help desk, to demonstrate best practices and to build confidence with the device.

Operational Risks

Other tasks assigned to senior management by the guidelines include the need to "understand operational risks and ensure that appropriate policies, procedures, and other controls are in place to mitigate them, including physical and logical access controls over RDC systems, original deposit items at customer locations, electronic files, and retained nonpublic personal information" (FFIEC, 2009).

In addition to having proper procedures and access controls in place, financial institution executives must also address the physical use of scanners and handling of paper checks. The FFIEC report highlights the following potential issues that may arise:

> 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. 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. 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 (FFIEC, 2009).

The report states that image quality can affect risk within the system, as well as faulty equipment due to a flawed design, regular "wear and tear" or intentional tampering. These issues can be avoided by having a tight link between the check scanner, API and software application since these relationships cannot be easily tampered with or hacked. Utilizing remote device monitoring can help mitigate risks associated with wear and tampering.

The guidelines also advise that one way to avoid potential risk problems is to only select third-party technology providers that have a reputation for reliability, high quality service and support and fault-tolerant, easy-to-use products.

Digital Check's small business check scanner, CheXpress© CX30, provides an optional rear ink jet printer that can be used to mark the back of the physical check as electronically deposited to a specific bank, but also to uniquely identify each check with a date and transaction number. These measures simplify the process of identifying an exception check when working with customers. Unlike a franking stamp that can stop working or be mechanically defeated, the presences of the ink jet data can be verified automatically via image processing (OCR) in Digital Check's API.

Poor image quality can lead to delays in processing checks as well as the potential of having checks rejected by the paying bank – a problem that exposes the bank of first deposit to potential losses. In order to reduce or prevent this risk, Digital Check offers unique thresholding and exception image processing in its API. Captured and thresholded images are immediately IQA tested against FSTC image quality standards and four additional parameters developed by Digital Check.

A new option has been added to detect and rotate documents scanned upside down. This option reduces the need for replacement documents since items with torn edges can be read upside down instead of having to use a carrier or replacement document.

To help software partners and ultimately banks create the best images possible from the Digital Check scanners, the company provides a simple interface feature to its API called DCCScan. DCCScan helps customers access the full functionality of the scanners by providing them with an optimized default configuration setting.

Technology-Related Risks

The guidelines call for appropriate technology and process controls such as bank-quality scanners. It warns that "information security risks may extend to the financial institution's own internal networks and networks of its service providers. These technology-related operational risks include failure to maintain compatible and integrated IT systems between the financial institution, service providers, and the customer" (FFIEC, 2009).

Selecting scanners from a reputable provider with a time-tested record of service, paired with the use of an API that gives financial institutions control over their environments provides additional control to the RDC process. Remote monitoring with Digital Check is fully supported by the API and by third parties such as Silver Bullet Technology, a provider of check scanning hardware and software.

Fraud Prevention

Another issue the guidelines address is fraud. With the deposit process happening outside of the financial institution, fraud prevention is, and should be, of great concern to financial institutions. Possible fraudulent activities are listed below:

> 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. Similarly, forged or missing endorsements, which may be detected by human inspection, may be less easily detected in an RDC environment. Certain check security features may be lost or the physical alteration of a deposited check – such as by "washing" or other alteration techniques – may be obscured in imaging or electronic conversion processes. Counterfeit items may be similarly difficult to detect. Duplicate presentment of checks and images at the institution or another depository institution represents both a business process and a fraud risk. 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. Access by customers and their staffs to nonpublic personal information contained on, or represented by, deposit items may also increase the risk of identity theft (FFIEC, 2009).

Digital Check scanners use magnetic ink character recognition (MICR) readers coupled with optical character recognition (OCR) to ensure checks are read correctly. The API flags any non-MICR items for the application to screen further.

The rear audit trail ink jet printer provides for item-level control of checks captured and helps reduce the resubmission of checks associated with operator error. The CheXpress© CX30 supports a rear ink jet printer that can be used to uniquely identify each check with date and transaction control information. Bank personnel can refer to these unique control numbers versus trying to describe to which check the bank or customer is referring. This number system simplifies the process of identifying an exception check when working with customers. Unlike a franking stamp, the presence of the ink jet data can be verified automatically via image processing in the DCC API at time of capture.

Deposited items can be marked, franked or otherwise noted as already processed by the CheXpress© CX30 to strengthen document control. The ink jet printer audit trail and franking mark (CX30 only) makes it clear that the item has been deposited.

Reputation and Oversight

A financial institution's reputation is closely tied to that of its technology and service providers. The guidelines recommend the following when selecting a service provider: "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 " (FFIEC, 2009).

Choosing a technology partner such as Digital Check that has been in business for more than 50 years, is a leader in RDC scanners and has a reputation for high-quality service, support and products places banks in a favorable position.

Maintaining control in the RDC process involves reviewing procedures regularly. The report recommends the following:

> Financial institutions should develop and implement risk measuring and monitoring systems for effective oversight of RDC activities. Institutions should ensure that customers using RDC have implemented operational and risk monitoring processes appropriate to their choice of technology…Effective management oversight involves regularly reviewing the reports and periodically conducting reviews and operational risk assessments. This will help ensure that the monitoring and reporting process accurately reflects current policies and procedures and sound practices (FFIEC, 2009).

In order to establish sound risk management and mitigation systems, Digital Check scanners give developers extensive control of the capture process via the API for tighter controls and fraud mitigation. As discussed above, Banks can create very tight controls over the RDC process. This information provides an additional audit trail to be captured and tracked with each scan.

One final benefit of having a rear audit trail physically printed onto the processed check is that the date of processing is printed on the back of the check making it easier for the user to track when the document should be destroyed. Banks may differ in their rules as to document retention and destruction; however, all banks agree that the original document should be destroyed within a specified time period after processing to prevent surreptitious representment of the check. Therefore, having an audit trail on the back with the date of processing can assist that process.

In closing, financial institutions must take a proactive stance to mitigate risk in all its forms in the remote deposit capture process. Arming yourself and your small business customers with scanners that address *all* of the attributes discussed in the FFEIC's guidelines is the best hedge against problems in the future.

References

Federal Financial Institution Examination Council. (2009). *Risk Management of Remote Deposit Capture*. Arlington, VA: U.S. Government Printing Office.