Country Club Bank
epcor Electronic Payments Core of Knowledge
PAYMENTS INSIDER
The inside scoop on payments for businesses of all sizes

Identifying Risks and Mitigation Techniques for RDC Commercial Users

by Caitlyn Mullins, AAP, APRP, NCP, Manager, Audit Services, EPCOR

Remote Deposit Capture (RDC) is a deposit transaction delivery system that allows an organization to send deposit documents from remote locations via image-capturing software to the organization's financial institution. An organization uses its financial institution's RDC software, and a scanner connected to a computer at its on-site location or a mobile device, to take an image of the check.

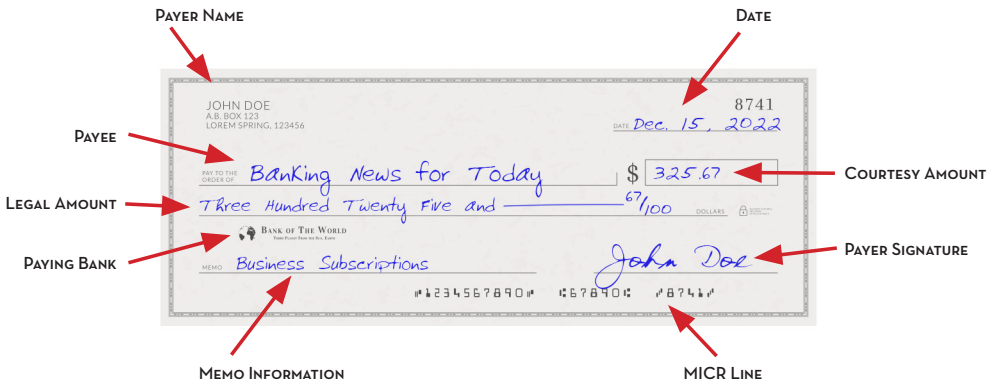
If you're a corporate user of RDC services, there are multiple risks that you are responsible to mitigate. Mitigating these risks by implementing strong controls and procedures can ensure the safety and security of your own organization, as well as aid in your financial institution's risk management program.

So, how do you introduce risk mitigation techniques? The first step is to educate staff on check basics, how to read a check and how settlement occurs.

Reading a Check

Here's a breakdown of check lingo, what each term means and where you can find the information on a check.

- **Payer Name:** Party ordering the payment.
- **Date:** The check must not be processed for settlement prior to the date written on the check.
- **Payee:** Party receiving the payment. Checks must be made payable to the organization's name.
- **Legal Amount:** Written in words.
- **Courtesy Amount:** Written in numbers—in the event the courtesy amount does not match the legal amount, you must uphold the legal/written amount.
- **Payer Signature:** The signature of the authorized signer of the payer account must be present.
- **Paying Bank:** Institution holding the Payor's account.
- **Memo Information:** Optional field that may give you more information about the payment.
- **Magnetic Ink Character Recognition (MICR) Line:** Descriptive check information comprised of numbers and symbols printed in the specific font that allows the check to be processed for settlement.
- **Endorsement (Not Pictured):** The payee must endorse the back of a check. Most financial institutions require a restrictive endorsement of imaged checks by writing "For Mobile Deposit Only at Financial Institution" with the deposit date, MM/DD, YY.



Settlement

Although your financial institution may credit your account the same day or the next day after you make your check deposit, this doesn't mean the checks have cleared settlement. Once your financial institution receives your deposit, they send those items/check images to their operator, who receives the images and then the checks are dispersed to the respected paying institutions. The paying institutions post the checks, or, if the check is unable to be processed, return the check back to your depositary institution. Depending on your financial institution's policies and procedures, the actual settlement process of individual checks can take several days.

Risks

Understanding the risks associated with RDC processing will allow you and your staff to identify and implement risk mitigation techniques.

- **Credit**—Credit risk arises when a party will not settle an obligation for full value. Checks can be returned by the payer's institution because of insufficient funds, a closed account, a stop payment order, forgery, fraud or other payment irregularity. To mitigate credit risk, management should establish appropriate risk-based guidelines to monitor returned items, recognize deposit limits, establish returned check procedures and disclose returned check policies to the payor.
- **Fraud**—Risks can arise with the RDC product when fraud is perpetrated by employees or by external sources. An organization is exposed to the risk of fraud when a wrongful or criminal deception leads to a financial loss for one of the parties involved. The risk of fraud can be managed effectively with the use of security controls, fraud monitoring tools and training to identify fraudulent items. Check fraud is on the rise, and it is crucial to train staff on how to detect and mitigate fraud.
- **Operational**—Operational risk may arise from the organization failing to process a transaction properly, having inadequate controls, an employee error, a computer malfunction, natural catastrophe, internal or external fraud, etc. Operational risks can be mitigated with policies and procedures, security controls and business continuity planning.
- **Legal and Compliance**—Legal and compliance risk arises from failure to comply with statutory or regulatory obligations. Safeguards must be in place for compliance with existing consumer protection statutes, regulations and state laws. Legal and compliance risks can be mitigated by regulatory and consumer protection obligations, commercially reasonable agreements and audit requirements. Additionally, management should provide payors with appropriate disclosures of the organization's policies.
- **Due Diligence and Suitability**—Management should establish appropriate risk-based guidelines to qualify and monitor employees with access to RDC software. For new and existing employees, a suitability review should involve consideration of the employee's job functions, trustworthiness and education. Due diligence and suitability risks can be mitigated by background checks on employees, annual reviews, ongoing education and vendor management procedures.
- **Information Security**—Organizations must evaluate the information technology and information security risks associated with RDC. Organizations must adjust their information security programs considering any relevant changes in technology, the sensitivity of client information, internal or external threats to information and their own changing business policies. Information security risks can be mitigated by adequate physical and logical assessment controls, and a business continuity plan that addresses RDC activity.

Risk Mitigation Techniques

Implementing Security Controls:

- Complex usernames and passwords for each staff member authorized to use RDC software.
- Restricting access to RDC software to only necessary staff.
- Performing background checks on staff with access to RDC software.
- Updating all software on a consistent basis.
- Implementing dual controls.
- Secure storage and disposal of check items.
- Deposit limits (including number of items and amount).

Periodic Training on Important Topics:

- RDC software procedures.
- Your financial institution's policies and procedures.
- Basic check knowledge.
- Current applicable laws and regulations.
- Current fraud trends.
- Identifying fraudulent checks.
- Identifying common security features of checks, including:
  - ⇨ Watermarks & security threads.
  - ⇨ Microprinting and holograms.
  - ⇨ Chemical reactivity and security inks.

Other Risk Mitigation Techniques:

- Periodic maintenance of scanner equipment.
- Ensuring all software is updated.
- Malware/virus protection.
- Business continuity planning.
- Vendor management policies and procedures.
- Monitoring reports.
- Establishing returned check procedures.
- Disclosing returned check policies and fees to the payor.

An organization utilizing RDC services should develop adequate policies and procedures that address the specific risks associated with RDC activity, including security procedures, monitoring system-generated reports, ongoing education, fraud monitoring, audit standards and due diligence practices. Understanding RDC processing and how to identify, as well as mitigate, risks will ensure your organization is getting the most out of your services.

Interested in having expert eyes on your organization's RDC program? Reach out to EPCOR at advisoryservices@epcor.org for more information and a free, no-obligation quote.

Electronic Payments Core of Knowledge

EPCOR is a not-for-profit payments association which provides payments expertise through education, advice and member representation. EPCOR assists banks, credit unions, thrifts and affiliated organizations in maintaining compliance, reducing risk and enhancing the overall operational efficiency of the payment systems. Through our affiliation with industry partners and other associations, EPCOR fosters and promotes improvement of the payments systems which are in the best interest of our members.
For more information on EPCOR, visit www.epcor.org.

Nacha® Direct Member

The Nacha Direct Member mark signifies that through their individual direct memberships in Nacha, Payments Associations are specially recognized and licensed providers of ACH education, publications and advocacy.

www.epcor.org
2345 Grand Blvd., Ste. 1700, Kansas City, MO 64108
800.500.0100 | 816.474.5630 | fax: 816.471.7665