epcor
Electronic Payments Core of Knowledge

PAYMENTS INSIDER

The inside scoop on payments for businesses of all sizes

INSIDE THIS ISSUE

Identifying Risks and Mitigation Techniques for RDC Commercial Users .... pg. 1
A Payments Fraud Carol .... pg. 4
A FAST Comparison of Faster Payments Options .... pg. 5
Give the Gift of Payments Resources .... pg. 6

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.

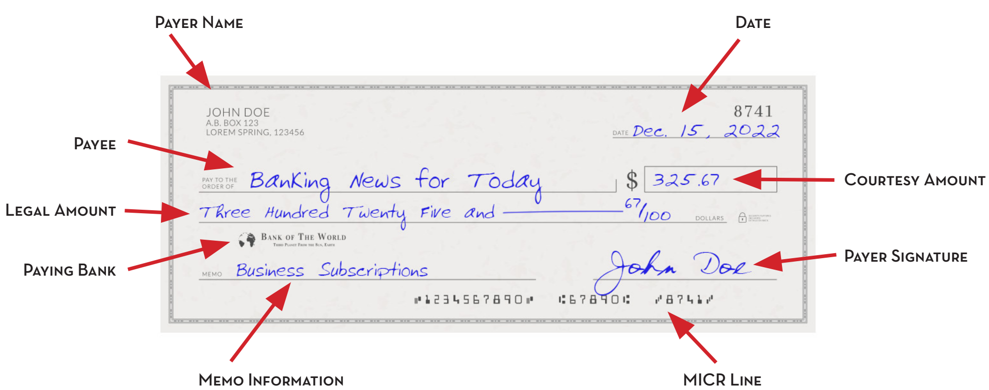
If you're a corporate user of RDC services, there are multiple risks that you are responsible to mitigate. Mitigating these risks by implementing strong controls and procedures can ensure the safety and security of your own organization, as well as aid in your financial institution's risk management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

<u>Implementing Security Controls:</u>

- 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).

<u>Periodic Training on Important Topics:</u>

- 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.

A Payments Fraud Carol

by Emily Nelson, AAP, NCP, APRP, Manager, Payments Education, EPCOR

The holiday season is officially upon us which also means it's time to reflect. In Charles Dickens' novella, *A Christmas Carol*, the ghost of Christmas Past represents the mind and its memories, the ghost of Christmas Present represents generosity, empathy and Christmas spirit while the ghost of Christmas Yet to Come represents the fear of death or moral reckoning.

Let's take a page out of Dickens' playbook and look at the ghosts of holiday scams past, present and future.

The Ghost of Holiday Scams Past

The Ghost of Holiday Scams Past presents itself as something familiar. We've seen it before and it's important that we remember what the consequences were for those types of scams.

Some of the more familiar scams of holidays past include fraudulent charities, social media ads linking to fake websites or even impersonation of well-known brands. Of course, the biggest repercussion of scams of any kind can be the loss of the funds transmitted. However, the other impacts often include a loss of trust in reputable brands or individuals trying to do good deeds each holiday season.

Rather than letting scammers get you down, focus on what you can do in the present to protect yourself and your funds.

The Ghost of Holiday Scams Present

The ghost of holiday scams present lurks on our holiday spirit and generosity. Let's shift our focus to how we can protect and maintain our holiday spirit and generosity. When donating to charity, we should exercise caution, whether you're the donator or the charity itself.

One way to ensure legitimacy *before* donating would be to check the URL or use the Better Business Bureau's Wise Giving Alliance or Charity Navigator. For any GoFundMe campaigns, you should consider researching the campaign manager before submitting the donation.

If you're part of a charitable organization accepting donations, consider how you advertise for donations. Perhaps your social media pages could include a secure link to your landing page for donations or try to use a clear path to your donation pages. This is just one example of how to protect ourselves both from the consumer and non-consumer perspective so that we are able to maintain our charitable spirit all season long.

The Ghost of Holiday Scams Yet to Come

Our ghost of holiday scams yet to come focuses on our fear of the unknown. However, we are going to focus on what we can practice today and implement in the future to reduce our fear of the things yet to come. Here are a few tips:

- **Practice good cybersecurity** by not clicking on links in ads or in emails from unfamiliar senders.
- **Pay close attention to anyone asking you to update information.** If an entity is asking you to update information via email or text, look up their contact information on your own and call them directly. If you are an entity needing to obtain updated information, consider how you are requesting the information from your consumer. Make sure you send them notices in advance or consider confirming information on file when they call in.
- When online shopping, stay safe by **confirming the URL contains an "https" address**.
- When buying from a seller online, **check their feedback rating from others**. This information can usually be found through a Google search. If it isn't, that may be a red flag. If you are an online merchant, **consider offering incentives** to ensure you are receiving feedback that can be shared with others.
- **Do not buy from sellers posing as authorized dealers** in areas in which no such product or deal would be applicable.
- **Be careful when purchasing from foreign countries.** If the seller makes requests for specific types of shipping that would avoid customs or if the seller is listed in the U.S., but the seller states they are out of the country for business or family.
- When purchasing online **consider using a credit card and monitor your statements regularly**.

- Avoid purchasing with pre-paid gift cards by giving the card numbers to the seller in an **unsecured manner**.
- **Never wire money for purchases.**
- Always **monitor the shipping process** for items purchased. There are also scams involving fake tracking information, so be mindful of this possibility and take action if something appears off. As a seller ensure you notify the purchaser of the shipment information in a timely manner and respond to any questions promptly.
- As a seller, **be leery of credit card purchases in which the shipping address and the delivery address vary greatly** in geographical area.
- **If it seems too good to be true, it probably is!**

While scams surrounding the holiday season are extremely common year after year, practicing the tips above during the present holiday scams season (and throughout the year) can save you and your organization from losing funds.

For more information regarding practices to protect you this holiday season take a look at the [FBI's holiday scams article]().

"Did You Know" EPCOR Launched a Business-Focused Video Series?!

This new series is a subsection of EPCOR's popular *Did You Know* video series and focuses on protecting small businesses and helping them stay vigilant and protected. Topics covered so far include small business invoice fraud prevention, CEO executive impersonation scams and point of sale (POS) fraud prevention. Check out the series on YouTube and subscribe so you don't miss an upload!

A FAST Comparison of Faster Payments Options

by Sharon Hallmark, AAP, Director, Payments Education, EPCOR

Faster payments provide greater convenience and efficiency for individuals and businesses by enabling the instant, or near-instant, transfer of funds. This speed helps in time-sensitive situations, such as paying bills, making urgent purchases or settling financial obligations promptly. This payment type also reduces reliance on traditional paper-based methods, like checks, which can be slow and cumbersome. By embracing electronic transfers, businesses can streamline their operations and reduce administrative costs.

According to the Faster Payments Council's *Faster Payments and Financial Inclusion* whitepaper, when it comes to financial inclusion, faster payments also provide easier access to banking services for underserved populations. The ability to send and receive money quickly and securely enhances economic participation and supports economic growth. They also have the power to bolster the overall economy by improving cash flow and liquidity management. Businesses can better manage their working capital, optimize supply chains and make informed investment decisions, ultimately driving economic productivity.

Faster Payments Network Rails

	Payment Type (Monetary transactions)	Settlement Timing	Transaction Limits	Amount/Type of Information with Payment
Same Day ACH	Push, Pull	Same Day	\$1,000,000	Up to 799,920 Characters
RTP® Network	Push	Immediate 24/7/365	\$1,000,000	Unlimited Characters via Extended Remittance
FedNow® Service	Push	Immediate 24/7/365	\$500,000	4,000 Characters
Visa Direct	Push	Same Day or Next Day	\$50K per OCT transaction \$100K/day (150 txn limit) \$250K/week (250 txn limit) \$500K/month (750 txn limit)	Varies by Case
Mastercard Send	Push	Same Day or Next Day	P2P: \$10,000 A2A: \$25,000 B2C: \$50,000	Varies by Case

So, what are your options for faster payments?

Faster payments include Same Day ACH, instant payments and push-to-card options. The two instant payment options are The Clearing House's RTP® Network and the Federal Reserve's FedNow® Service. The two push-to-card options are Visa Direct and Mastercard Send.

Now, let's look at what differentiates these faster payment options.

The choice of a faster payment option depends on various factors and can vary based on individual preferences and specific requirements. Here are a few considerations to help you decide what's right for your organization:

1. **Speed:** Different payment options offer varying levels of speed. Assess the urgency of the transaction and

choose a payment method that aligns with your desired timeline. Some options provide instant or near-instant transfers, while others may take hours or even a day.

2. **Accessibility:** Consider the availability and accessibility of the payment option. Determine if the receiver has access to the chosen payment system or platform. It's essential to ensure compatibility between the sender and receiver's accounts.
3. **Transaction limits:** Check if there are any transaction limits or restrictions associated with the payment option. Some methods may have limits on the amount you can transfer, which could impact your decision if you're dealing with larger sums of money.
4. **Cost:** Evaluate the fees associated with each payment option. Some methods may charge transaction fees, while others offer free or low-cost transfers. Consider the cost implications and choose an option that aligns with your budget and cost-effectiveness.
5. **Security:** Ensure the chosen payment option provides robust security measures to protect your financial information and transactions. Look for encryption, authentication protocols and fraud prevention measures.
6. **Integration:** Evaluate if the payment option integrates well with your existing financial systems. Seamless integration can simplify payment processes and enhance efficiency.

It's important to assess these factors based on your specific needs and priorities. It's also helpful to keep up with the latest developments in the payment industry to stay informed about new and emerging faster payment options.

And remember, your financial institution is your biggest cheerleader and will be there to help you along the way! Reach out to them and they will be happy to help you decide what is the right option for your organization and situation.

Give the Gift of Payments Resources

by Madison Howard, Manager, Member Communications, EPCOR

It's that time of year again—the halls are decked, the New Year is coming and you can't go anywhere without hearing Mariah Carey!

This is the time of year when many organizations begin looking ahead to the new year, finish finalizing their budget plans and set new goals for the year ahead. Plus, with many organizations seeing vital staff members approaching retirement, it's imperative to identify ways to educate less-tenured staff to take their place.

The best way to be successful is to have the right tools and education. So, grab your hot chocolate and your coziest (or ugliest) holiday sweater, because *Mariah Carey voice* it's *TIIIIIMEEEEEE* to look at payments education gifts for your staff and clients!

ACH Rules

What better way to ensure compliance with the *ACH Rules* than to provide access to the *ACH Rules*? Consider reaching out to your financial institution if you need a copy, or additional copies.

ACH Quick Reference Guide for Corporate Users

EPCOR's *Guide* is a quick summary of all the *Rules* ACH Originators need to know and covers general rules, ODFI/ Originator requirements, prerequisites and warranties, as well as a review of all the processes such as returns, NOCs, prenotes and more!

Did You Know… Informational Videos

These quick and free animated videos explain payments topics in just a few short minutes! The fun format and easy-to-understand language make these videos perfect for passing along important information to staff and clients. Recent topics include business email compromise (BEC scams), AI payments scams, ATM fraud and more. EPCOR also recently launched a business-focused series that concentrates on protecting small businesses and helping them stay vigilant and protected. Topics covered so far include small business invoice fraud prevention, CEO executive impersonation scams and point of sale (POS) fraud prevention. These videos are available on EPCOR's website, LinkedIn and YouTube channel.

Payments Insider

Payments Insider (which you're reading now) is an e-newsletter released four times a year (once per quarter) and is designed to inform businesses of all sizes of recent payment systems developments. The latest copy of this newsletter is always available on the Corporate User Webpage.

Corporate User Webpage

This webpage contains end-user resources, information on upcoming *ACH Rules* changes and much more. New resources are constantly being added and suggestions from page visitors are encouraged. Visit the webpage at epcor.org/corporateuser.

Third-Party Sender Webpage

This webpage contains sample agreements and tools, educational videos, links to helpful *Workbooks* and more. Visit the webpage at epcor.org/tpsuser.

If you have any questions or aren't sure what resource is right for you or your organization, reach out to your financial institution. Happy holidays!

BANK of
BELLEVILLE • CLINTON COUNTY
MADISON COUNTY • MONROE COUNTY
Smaller Bank • Bigger Service • Stronger Community

epcor®

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