Payment & Deposit Risks on the Radar

Risk Management Insights

Payments & Deposits

Focused on helping credit unions manage risks related to payment and deposit transactions.

The Impact of a Constant-Evolving Fraud Environment.

With the evolving payments landscape and increase in fraud, protecting your credit union has become more challenging. Emerging risks like account takeovers, synthetic ID fraud, alternative payments, and more are forcing credit unions to think differently. Fraudsters continue to find new ways to perpetrate fraud, but you can stay one step ahead by implementing appropriate controls.

1:1 Payment and Deposit Q&A with a Risk Consultant

Question: Does the Remote Deposit Capture (RDC) Indemnity in Regulation CC (Reg CC) require the use of restrictive endorsements on paper checks prior to transmitting the images for deposit to our credit union?

Risk Consultant: No, the indemnity provision does not require RDC users to restrictively endorse the paper checks; however, a best practice is for credit unions to minimize the risk of indemnity claims by requiring restrictive endorsements – such as "For Mobile Deposit Only to ACB Credit Union" - and to reject checks lacking restrictive endorsements.

The RDC indemnity provision is designed to reduce losses from duplicate presentments by protecting a depositary institution that accepts a paper check for deposit that is returned unpaid to that institution due to being previously deposited to another institution via RDC. However, the indemnity does not apply if the paper checks are restrictively endorsed.

Question: What are your recommendations for qualifying members for RDC?

Risk Consultant: A common practice is to evaluate creditworthiness and ChexSystems data to qualify members for RDC service. You can combine this with other criteria, such as length of membership and deposit and loan relationships.

Qualifying businesses for RDC should be based on a review of financial statements and/or tax returns. Updated financial statements and/or tax returns should be reviewed on an annual basis thereafter to detect negative changes in financial condition. Negative changes should result in re-evaluating the business member's RDC limits or their continued eligibility to participate in the RDC program.

Some credit unions qualify members for RDC based on length of membership (e.g., 60 days) and whether the account is in good standing. This criterion is not always a good predictor of how members will use RDC.

Ken Otsuka, Senior Risk Consultant | Risk & Compliance Solutions

Proactively supporting credit union risk management and compliance efforts, dedicated Risk Consultants are available to assist you credit union in managing risks and helping you make strong strategic decisions. **C**ontact CUNA Mutual Group's Risk Consultants at **800.637.2676** or riskconsultant@cunamutual.com

10007788-0718 © 2018 CUNA Mutual Group, All Rights Reserved.

1:1 Payment & Deposit Q&A with a Risk Consultant

Question: Does checking the preprinted check box, For Mobile Deposit Only, on the back of the check count as a restrictive endorsement?

Risk Consultant: While a number of check vendors have added a checkbox on the back of checks indicating "for mobile deposit only," it is our position that checking this box does not count as a restrictive endorsement. The idea behind a restrictive endorsement is to restrict the negotiation of the check to the credit union only.

The restrictive endorsement should include:

- "For Mobile Deposit Only to ABC Credit Union,"
- Account number –optional for privacy purposes, and
- The member's signature

Question: How can we manage the risk from fallback transactions?

Risk Consultant: Fallback transactions occur when a chip-enabled terminal is unable to read the EMV chip so the transaction is completed using the magnetic stripe. There are a number of reasons for fallback transactions – such as, merchant hardware/software not properly installed or a dirty or damaged chip to name a few. However, fallback transactions can also occur when a fraudster creates a counterfeit magnetic stripe card with an intentionally damaged chip. You can manage this risk by working with your card processor to develop rules for fallback transactions at POS terminals and ATMs based on data points, such as transaction amount, geolocation, merchant category code, etc., that fit your credit union's risk appetite.

Question: What types of risk mitigation tools should be in place for card-not-present transactions?

Risk Consultant: These risk mitigation tools should be in place to help manage card-not-present fraud:

- Address Verification Service
- Visa's CVV2 / Mastercard's CVC2
- Verified by Visa / Mastercard Secure Code

An exciting tool on the horizon is technology referred to as Dynamic Code Verification (DCV). DCV is similar to CVV2 / CVC2 except that the DCV code changes over time, such as every hour.

Question: What is the ACH booster payment scam on credit cards? What risk mitigation steps do you recommend?

Risk Consultant: When a member makes an ACH payment via ACH debit, funds are pulled from an account at another financial institution (Receiving Depository Financial Institution or RDFI) to apply to the member's credit card account. ACH booster payments is a scheme to pay down the balance on a card to free up credit limit, which the member immediately uses up through cash advances before the ACH debit is returned unpaid by the RDFI. The returned payments are charged back to the credit card account. Credit unions are not discovering the fraud in a timely manner which can result in card balances that significantly exceed the approved limit on the cards.

Mitigate the risk of ACH booster payments by adopting these controls:

- Limiting the payment frequency of ACH payments in a billing cycle, such as 1 payment per rolling 5- or 7-day period.
- Delaying the availability of the credit limit freed up by the ACH payment. Under Regulation Z, credit unions must post the payment as of the date of receipt for the purpose of computing finance charges, but there is no requirement to provide immediate availability to the credit limit that is freed up from the payment.
- Generating and reviewing large payments, returned payments, over limit and credit balance reports daily.
- Determine if the processor provides an excessive payment activity report and ACH daily payments and returns report. These reports should be reviewed daily. And,
- Train tellers to be on the look-out for members who request frequent cash advances in a single month or billing cycle.

Note: ACH booster payments can also be made on other line-of-credit loans a member may have.

Access Payment & Deposit resources in the **Protection Resource Center** at **www.cunamutual.com/prc**

1:1 Payment & Deposit Q&A with a Risk Consultant

Question: Our credit union has experienced large losses from counterfeit checks drawn on HELOCs as well as members' checking accounts. What risk mitigation strategies are recommended?

Risk Consultant: Losses involving counterfeit checks drawn on member accounts, particularly HELOCs, are increasing. In fact, counterfeit HELOC checks have ranged from $25,000 to as much as $350,000. Other large losses involve counterfeit checks drawn on member checking accounts that are funded with unauthorized advances against member HELOCs.

Credit unions should consider performing a manual review of large dollar items drawn on the credit union that are presented for payment. You can establish a monetary threshold for this purpose, such as reviewing items greater than $50,000. Verify the member's signature as drawer against the signature card. If the signature is in doubt, consider calling the member to confirm he or she issued the check to the named payee in the amount specified. The review would have to be timely so that you can return any unauthorized checks by your midnight deadline.

If a counterfeit check clears the member's account and you are unable to return it by your midnight deadline, you can attempt to recover the loss by sending the counterfeit item "without entry" to the institution where it was deposited requesting reimbursement. In sending the counterfeit item "without entry," the credit union mails a copy of the check along with the member's forgery affidavit with a letter asking for restitution. An indemnification agreement may be requested by the depositary institution. The credit union must exercise its own discretion in whether or not to provide the indemnification.

The depositary institution may not honor the credit union's request to recover the funds citing the UCC's midnight deadline. However, some institutions will assist credit unions by returning the available funds in the account up to the amount of the check.

Question: What consumer protection regulations apply to unauthorized transactions using mobile wallets?

Risk Consultant: To determine which consumer protection regulations apply, if any, you must determine whether the mobile wallet is linked to a debit card/checking account or a credit card:

- Regulation E applies when the mobile wallet is linked to the user's debit card/checking account.
- Regulation Z applies when the mobile wallet is linked to the users credit card.
- Visa/Mastercard zero liability provisions may apply.

Funds Stored on the Mobile Wallet App

It becomes more complicated when funds are stored directly on the mobile wallet app. There is no protection for users from unauthorized use of a mobile wallet that results in funds being transferred directly from the app and the credit union is not obligated to refund the loss.

However, if there is unauthorized funding to load / reload the mobile wallet app resulting in unauthorized transfers to other parties, Regulation E or Regulation Z applies depending on whether the app was loaded / reloaded via debit card / checking account or credit card, respectively.

Risk & Compliance Solutions • 800.637.2676 • riskconsultant@cunamutual.com

This resource is for informational purposes only. It does not constitute legal advice. Please consult your legal advisors regarding this or any other legal issues relating to your credit union. CUNA Mutual Group is the marketing name for CUNA Mutual Holding Company, a mutual insurance holding company, its subsidiaries and affiliates. Insurance products offered to financial institutions and their affiliates are underwritten by CUMIS Insurance Society, Inc. or CUMIS Specialty Insurance Company, members of the CUNA Mutual Group. CUNA Mutual Group Proprietary and Confidential. Further Reproduction, Adaptation or Distribution Prohibited.

800.637.2676 | cunamutual.com
P.O. Box 391 | 5910 Mineral Point Road
Madison, WI 53701-0391
10007788-0718 © 2018 CUNA Mutual Group, All Rights Reserved.

CUNA MUTUAL GROUP