

# RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.



CUNA  
MUTUAL  
GROUP

Alert Type

Awareness

Watch

Warning

## Liability for Wire Fraud Schemes Targeting Real Estate Closings

Credit unions and their members continue to be victimized in a wire transfer fraud scheme designed to steal the funds needed to close real estate transactions. Purchasers intending to pay for the property using their personal funds are particularly vulnerable to this scam. Upon finding an upcoming closing, fraudsters send a spoofed email containing “updated wire instructions” to the credit union / lender or the member/purchaser. If the member/purchaser is targeted and they wire their personal funds for the closing using the updated wire instructions, they may attempt to hold the credit union liable if the wire cannot be retrieved.

### Details

Misdirected wires have been the subject of litigation involving fraudulent wire instructions for real estate closings, which is related to the business email compromise scam. In this scam, fraudsters hack title company/closing agent’s email to search for upcoming real estate closings. When they find one, they frequently send a spoofed email to the purchaser containing “updated wire instructions” for the closing. (Alternately, the fraudster could send the fraudulent email from within the compromised email account).

Believing the updated instructions to be legitimate, the purchaser provides the wire instructions to their financial institution to execute the wire. Upon discovery of the fraud, the purchaser’s financial institution is generally unable to recover the funds from the beneficiary bank. The purchaser could file a lawsuit against the beneficiary bank or their own financial institution to recover the funds.

Possible outcomes:

- The purchaser’s lawsuit against the beneficiary bank would not likely succeed since UCC 4A-207 does not require a beneficiary bank to match the beneficiary’s name contained in the incoming wire to the beneficiary’s account. However, if the beneficiary bank is aware of the name mismatch, it assumes liability if it still credits the account of the beneficiary.
- The purchaser’s financial institution could be found liable for the misdirected wire if it did not properly disclose how wires can settle at the beneficiary’s bank.

Wire transfers are governed by model Article 4A of the Uniform Commercial Code (UCC 4A). [UCC 4A-207](#) (Misdescription of Beneficiary), establishes liability for misdirected wires. It provides that beneficiary banks are only obligated to match the account number contained in the incoming wire transfer (also referred to as a payment order) to the beneficiary’s account. In fact, a very large percentage of incoming wires at beneficiary banks are completely automated in that they are automatically credited to the beneficiary’s account using only the account number.

**Date:** January 18, 2022

**Risk Category:** Funds Transfer; Wire Transfer; Fraud; Scam; Liability; Real Estate

**States:** All

**Share with:**

- Compliance
- Executive Management
- Legal
- Loan Manager
- Loan Staff
- Risk Manager
- Transaction Services



**Facing risk challenges?**

[Schedule](#) a free personalized discussion with a Risk Consultant to learn more about managing risk.

# Liability for Wire Fraud Schemes Targeting Real Estate Closings

Under UCC 4A-207(c)(2), credit unions can shift liability for misdirected wires to members by disclosing, in writing, how wires settle at the beneficiary's bank. That is, on the basis of the beneficiary's account number even it identifies a person different than the named beneficiary. Members must acknowledge this disclosure item through their signature. The credit union would be liable for the loss in the absence of this liability shifting language.

This scam has also targeted credit unions that provide financing (e.g., mortgage loans) for the real estate closing. In these cases, the credit union's loan department receives the fraudulent email containing the updated wire instructions and wires the funds based on the fraudulent instructions. In this case, UCC 4A-207 places liability for the misdirected wire on the credit union lender.

Some credit unions may also be using electronic wire transfer agreements and/or electronic wire transfer request forms that are electronically signed by members. Any liability shifting language contained in the electronic wire transfer documents may not be legally enforceable since the federal E-Sign Act and state UETA laws do not extend to UCC 4A.

## Risk Mitigation

Credit unions should consider these risk mitigation tips:

- Ensure wire transfer agreements and wire transfer request forms disclose how wires settle at beneficiary banks. Ensure the language is closely aligned with the requirement in UCC 4A-207(c)(2). The following is sample disclosure language to consider:

If your payment order identifies the recipient and any financial institution by name and account or other identifying number, the Credit Union and any other financial institutions facilitating the transfer may rely strictly on the account or other identifying number, even if the number identifies a different person or financial institution.

- Avoid using electronic wire transfer agreements and request forms that are e-signed.
- Train frontline staff so they can warn members on this scam when members request a wire for a real estate closing. Staff should verify the updated wire instructions on behalf of the member using a reliable phone number.
- If the credit union's loan department receives an email purportedly from a title company/closing agent containing updated wire instructions for member loan closings, verify the instructions by calling the title company/closing agent using a reliable phone number.

## Risk Prevention Resources

Access CUNA Mutual Group's [Protection Resource Center](#) for exclusive risk and compliance resources (User ID and Password required).

- RISK Alerts: Access the [RISK Alerts Library](#) and enter "wire transfers" in the search feature
- [Wire Transfer Risk Overview](#)
- [Fraud & Scams eBook](#)
- [Business Email Compromise Risk Overview](#)



**Access the Protection Resource Center for exclusive resources:**

- [Loss Prevention Library](#) for resources & checklists
- [Webinars and Education](#)
- [RISK Alerts Library](#)
- [Report a RISK Alert](#)

The Protection Resource Center requires a User ID and Password.

© CUNA Mutual Group, 2022.

Insurance products offered to credit unions are underwritten by CUMIS Insurance Society, Inc., a member of the CUNA Mutual Group. This RISK Alert is intended solely for CUNA Mutual Group Fidelity Bond policyowners to prevent fraud losses. Any further distribution of this information could subject you to liability under common law and various statutes including the Fair Credit Reporting Act.

This resource was created by CUNA Mutual Group based on our experience in the credit union, insurance, and risk management marketplace. It is intended to be used only as a guide, not as legal advice. Any examples provided have been simplified to give you an overview of the importance of selecting appropriate coverage limits, insuring-to-value, and implementing loss prevention techniques. No coverage is provided by this resource, nor does it replace any provisions of any insurance policy or bond. Please read the actual policy for specific coverage, terms, conditions, and exclusions.