TruStage™

Money mule

Risk overview

Money mules are recruited by fraudsters to assist in laundering money obtained through illicit activities, such as money stolen from victims of fraud. In many cases, fraudsters recruit money mules with bogus job offerings through online job ads or social media with promises to earn easy money for minimal work. Money mules add layers of recipients to the money trail which complicates law enforcement's ability to track the money from the victims to the fraudsters.

Types of money mules

Typically, money mules fall within three categories:

- **Unwitting participants**
  These money mules are typically recruited through online job scams, won a sweepstakes, or strike up an online relationship and are unaware that they are engaged in criminal activity.
- **Witting participants**
  These money mules are aware that they may be involved in suspicious activity but engage in it anyway.
- **Complicit participants**
  These money mules are fully aware that they are engaged in criminal activity.

Money mules may open accounts under their own identity. Alternately, they may be instructed to open the accounts using a stolen or synthetic identity.

Money mules may be instructed to open an account, including business accounts, at a specific financial institution or use their own account to receive the funds. Fraudsters transfer funds from accounts of fraud victims to the money mule accounts. Upon receipt, the money mules are typically instructed to wire the funds elsewhere. Alternately, the money mules may be instructed to purchase cashier's checks, convert the money to virtual currency, purchase gift cards, or a combination of these actions.

Money mules are also recruited to cash stolen checks, such as U.S. Treasury checks. The money mules are instructed to open accounts, including business accounts, at financial institutions in the name of the payees listed on the checks to deposit the stolen checks and transfer the funds elsewhere.

Typical money sources

- Account takeovers
- Wire fraud, including business email compromise and related scams, such as vendor impersonation
- Online romance, job, or sweepstakes scam victims
- Other credit-push payment scams

Upon receipt of the funds, the money mules are instructed to transfer the funds elsewhere. The transfers may be to other money mules in the network or to accounts controlled by the fraudsters. The transfers may be by wire or ACH using external transfer service.

> Money mule solicitations are commonly disguised as work from home opportunities, usually to process payments.

Money laundering life cycle

Knowingly moving money for illegal activities can lead to serious consequences — including criminal charges. Money mules, however, typically move money at someone else's direction, not knowing that their activity benefits fraudsters. These individuals, even if they don't realize it, enable fraudsters to harm others.

Money laundering is the process deployed by fraudsters to disguise money derived from illicit activities.

There are three stages to money laundering schemes:

- **Placement**
  The first stage of money laundering is placement, which is the process of moving ill-gotten money from victims into the financial system and further away from its illegal source.
- **Layering**
  The second stage of money laundering is layering the purpose of which is to make the ill-gotten money as hard to detect as possible by moving it further away from its source.
- **Integration**
  The last stage of money laundering is integration where the ill-gotten funds are integrated into the legitimate financial system.

Money mules play a role in the placement and layering stages of the money laundering life cycle allowing the fraudsters to further distance themselves from source of the money.

Money mule accounts may increase litigation risk

A lawsuit was filed against a credit union by a business to recover $558k in stolen funds resulting from a vendor impersonation scam. The business received a spoofed email - appearing to come from a vendor used by the business – containing updated banking instructions for remittances. Following the updated instructions, the business initiated four ACH credit transfers totaling $558k that were deposited to a consumer-member's account (money mule) at the credit union. The member/money mule subsequently withdrew the funds.

The incoming ACH credit transfers contained the name of the vendor which did not match the name on the member/money mule's account. In addition, the SEC code on the incoming ACH credit entries was "CCD" (Corporate Credit or Debit), which is strictly reserved for commercial accounts.

Nacha rules along with UCC 4A-207 (Misdescription of Beneficiary) do not require credit unions as receiving depository financial institutions (RDFIs) to match the name on incoming ACH credit transfers to the name on the member/receiver's account. However, if a credit union becomes aware that the names don't match, the ACH credit entry – or incoming wire transfer - should be returned based on UCC 4A-207. The credit union argued that they were not obligated to determine if the names matched and that it had no knowledge of the name mismatch.

The credit union's system generated a real-time alert whenever the name on an incoming ACH credit transfer does not match the name on the member/receiver's account. However, the credit union did not review these alerts.

The court ruled in favor of the business by concluding that actual knowledge of the name mismatch can be imputed on the credit union because the transfers generated real-time alerts on the name mismatches. The credit union was ordered to return $558k to the business.

Money mule red flags

Credit unions should take proactive steps to detect suspicious/unusual transaction patterns that are indicative of money mule activity. Identifying money mule accounts starts with monitoring incoming transfers/payments to member accounts.

Some common money mule red flags include:

- Changes in transactional patterns for existing members, such as sudden large dollar incoming wires and/or ACH credit transfers that are immediately transferred out of the account.
- Large dollar incoming transfers (ACH and wires) to new member accounts followed by immediate transfers out of the account. Money mules can also purchase large dollar cashier's checks or by using debit cards to purchase gift cards.
- Large dollar incoming wire transfers where beneficiary's name contained in the incoming payment order does not match the name on the member's account.

  Note that Article 4A of the Uniform Commercial Code (UCC 4A-207, Misdescription of Beneficiary) does not require financial institution to match the name in incoming payment orders to the member's account; however, if the credit union is aware of the name mismatch, the wire should be returned to avoid liability.
- Large dollar incoming ACH credit transfers where the receiver/member's name contained in the ACH entry does not match the name on the member's account.

  Note that Nacha rules, as well as UCC 4A-207, do not require receiving depository financial institutions to match the receiver's name in the ACH entry to the name on the receiver/member's account. If the credit union is aware of the name mismatch, the ACH credit entry should be returned to avoid liability under UCC 4A-207.
- Large dollar incoming ACH credit transfers to consumer/receiver accounts where the SEC code contained in the ACH entry is CCD (Corporate Credit or Debit Entry) or CIE (Customer Initiated Entry). Consumer SEC codes (PPD, WEB, TEL) are used for entries to consumer/receiver accounts, while CCD and CIE codes go to commercial accounts.
- Large dollar member-to-member transfers from compromised member accounts to newer accounts.
- Rapid movement of funds through the account with little to no balance retention.
- Large dollar checks, including U.S. Treasury checks, deposited by new members followed by transfers out of the account after the check holds expire.

In situations where it is suspected that money mules are opening fraudulent business accounts and filing fraudulent articles of incorporation with the secretary of state to cash stolen checks, such as U.S. Treasury checks, credit unions should be on the lookout for:

- Articles of incorporation filed just days before the account is opened. In some cases, the articles of incorporation are filed the day before the account is opened.
- The payee's address listed on the check bears no relationship to the address used to open the account.

Money mules

Nacha rule changes

Nacha rule changes that were approved by Nacha members in early 2024 are designed to reduce the incidents of fraud that make use of credit-push payments. The rule changes have varying effective dates in 2024 and 2026.

The rule changes are intended to assist originators and originating depository financial institutions (ODFIs) recover losses from ACH credit transfers initiated due to fraud, such as in cases of account takeovers and when originators are fraudulently induced to initiate ACH credit transfers. The fraudulent ACH credit transfers are frequently deposited to money mule accounts.

One rule change requires receiving depository financial institutions (RDFIs) to implement risk-based processes and procedures to identify incoming ACH credit transfers initiated due to fraud.

Phase 1 requires RDFIs with an annual ACH receipt volume of 10 million or greater in 2023 to comply by March 20, 2026. Phase 2 requires RDFIs with an annual ACH receipt volume of less than 10 million in 2023 to comply by June 19, 2026.

Another rule change expands the use of return reason R17 for RDFIs to return an ACH credit entry that it believes to be fraudulent (effective date October 1, 2024).

How should we advise members that have been approached to become a money mule?

Educate credit union staff to encourage members that they should stop communicating with the person who asked them to send and receive money – that is, act as a money mule.

If the member currently has money in their possession from the activity, suggest that they shouldn't send it to the person who has been giving directions. They should report the communications and suspicious activity to law enforcement.

If the member provided any information to the person to whom they've been communicating with, they should closely monitor and scrutinize their accounts for suspicious transactions. If warranted, the member may eventually want to work with your credit union to change account details or adjust online banking set-up.

Can you remove, ban or expel members that knowingly become a money mule related to fraud and scams?

Yes, credit unions can expel a member serving as money mule by assisting fraudsters launder ill-gotten funds. Federal credit unions (FCU) can expel members in one of three ways:

- By a two-thirds vote of the members present at a special meeting to expel the member;
- Under a nonparticipation policy given to each member; or
- By a two-thirds vote of a quorum of the FCU's board of directors to expel the member "for cause."

The NCUA defines "for cause" as:

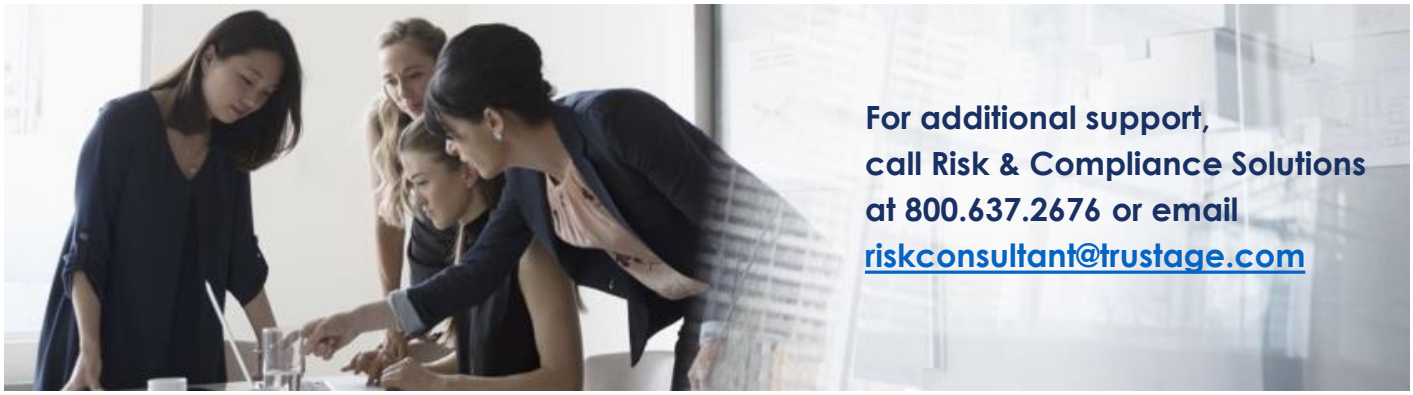
- A substantial or repeated violation of the credit union's membership agreement.
- A substantial or repeated disruption, including dangerous or abusive behavior, to credit union operations.
- Fraud, attempted fraud, or conviction of other illegal conduct in relation to the credit union, including the credit union's employees.

A credit union's board of directors may vote to expel a member "for cause" if the credit union provides the member a copy of Article 14 of the FCU bylaws (Appendix A to Part 701 of the NCUA's Rules and Regulations), or the optional standard disclosure notice contained in Article 14. Credit unions seeking to expel a member "for cause" must provide advance notice in writing along with the reason for expulsion (refer to Appendix A to Part 701 for more details).

If your credit union has a limitation of services policy, you can also limit services to a member who engages in fraudulent conduct.

Mitigation tips to fend off money mules

- Train staff on the role money mules play in laundering ill-gotten money along with the red flags that may be indicative of money mule activity.
- Deploy an identity verification solution that can detect synthetic identities to screen new member applicants.
- Deploy a real-time fraud monitoring solution with behavioral analytics that leverages artificial intelligence and machine learning to identify suspicious transactions that may be indicative of a money mule activity.
- Although credit unions are not required to match the name contained in incoming ACH credit transfers and incoming wire transfers to the name on the account, credit unions should consider generating a system alert whenever a name mismatch is detected. The alerts should be reviewed in a timely manner to allow the credit union to perform an investigation and return the ACH credit entry or wire, if necessary. These alerts will become particularly important for credit unions as RDFIs in 2026 when the Nacha rule for deploying risk-based processes and procedures to identify incoming ACH credit transfers initiated due to fraud go into effect.
- Be alert for mismatched SEC codes on incoming ACH credit transfers. The correct SEC code is determined by the intended receiver of the incoming ACH transaction. Consumer SEC codes (PPD, WEB, TEL) are used for entries to consumer accounts while CCD and CIE SEC codes should go to commercial accounts. A mismatched between a commercial SEC code and a consumer/receiver account may be indicative of money mule activity. While it may be common for a commercial account to receive a consumer SEC code (e.g., WEB debit), a new or large dollar commercial SEC code to a consumer/receiver account warrants additional scrutiny.
- Credit unions can return ACH credit entries using return reason code R17 if they believe the transfers were initiated due to fraud.
- Scrutinize new business accounts. Be alert for articles of incorporation that are filed shortly before the account is opened. If the check being deposited by a new business member contains the payee's address, make sure it matches the address used to open the account. Also, place extended holds on checks deposited by new business members.
- File a Suspicious Activity Report (SAR) when necessary.



For additional support, call Risk & Compliance Solutions at 800.637.2676 or email riskconsultant@trustage.com

TruStage