



Risk & Compliance Solutions | Webinar

Money mules & their schemes

Preventing the work of illicit actors

Proprietary and confidential. Do not distribute.



Today's panelists



Becky Garton
TruStage™
Risk Consultant
Wisconsin



Ken Otsuka
TruStage™
Senior Risk Consultant
Illinois



Brad Neumann
TruStage™
Senior Risk Consultant
Wisconsin

Money mule fraud serves as a form of micro-laundering run through smaller consumer accounts rather than disguised within the larger transactions.

Types of money mules

Unwitting

Typically recruited through online job scams or they're victims of a scam – like the romance scam – and are not aware they are engaged in criminal activity.

They genuinely believe they are helping their employer or someone posing as their romantic partner.

Witting

Are aware they may be involved in suspicious activity but engage in it anyway.

They ignore warning signs of criminal activity or are willfully blind to the financial activity they are participating in.

These individuals typically start as unwitting participants.

Complicit

Are fully aware they are engaged in criminal activity

Recognizing a money mule

Often recruited

- Money troubles
- Lack of financial knowledge
- Unfamiliarity with technology
- Desire for quick payout

Vulnerable

- Students
- Young adults
- Unemployed
- Elderly





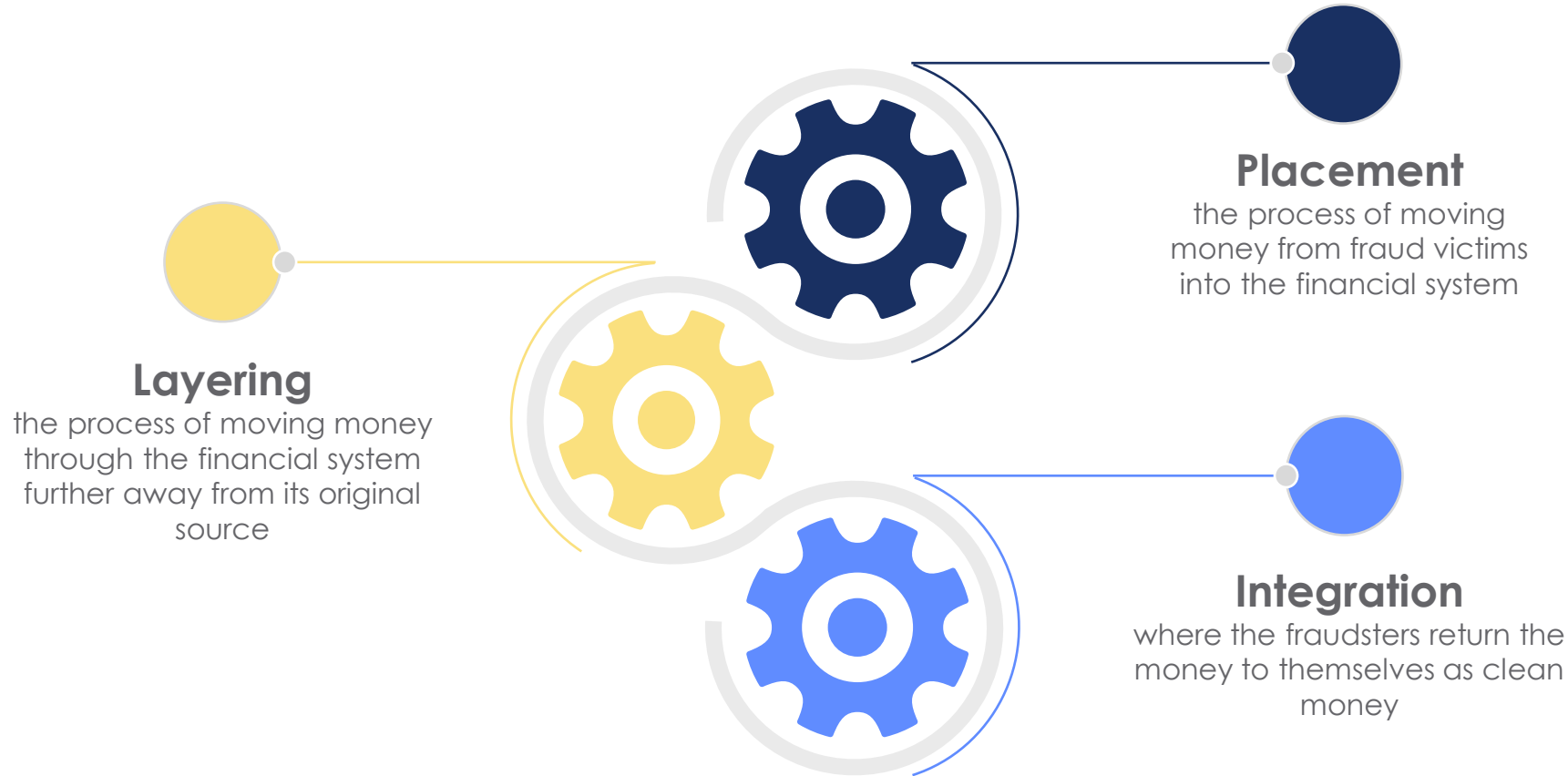
- **Social media outreach** with offers of easy money - fake job postings, direct messaging campaigns, and the creation of fraudulent business pages
- **Job advertisements** - fraudulent job listings with high salary offerings for minimal work, emphasizing remote work possibilities.
- **Phishing emails** with urgent requests for financial assistance, tricking individuals into providing personal information or accepting money transfer tasks

Once recruited, the money mule is familiarized with the task of transaction handling within the laundering process.

How are money mules recruited?

Money laundering life cycle

The process deployed by fraudsters to disguise money derived from illicit activities



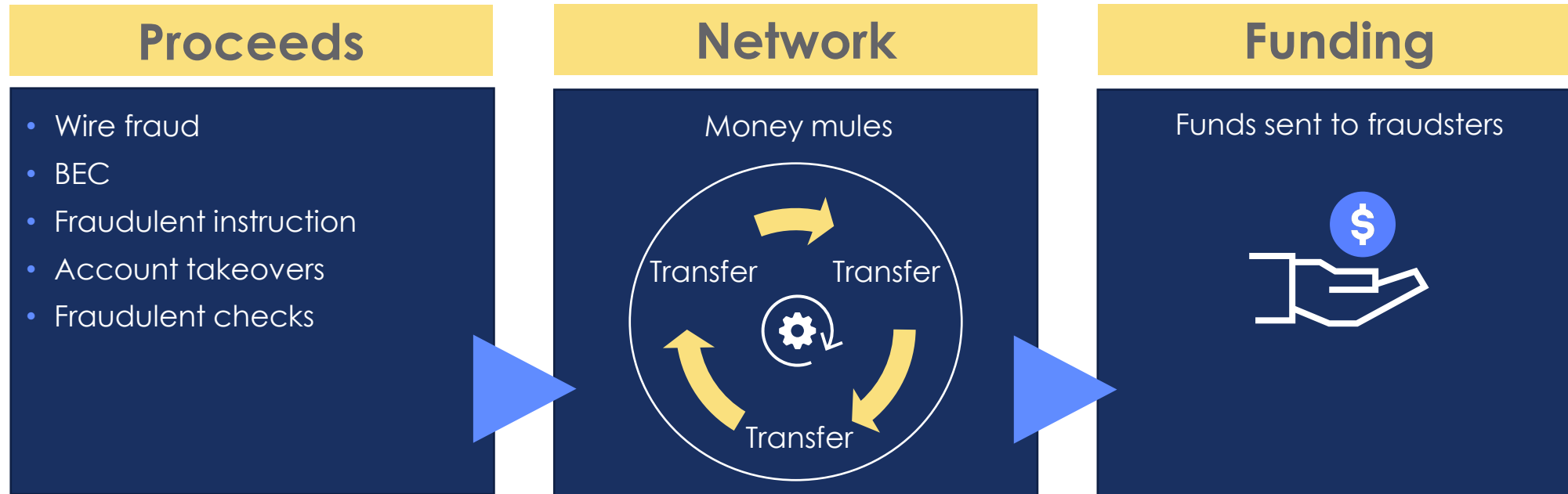
Typical money sources



- 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

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.

Money mule role in laundering stolen funds



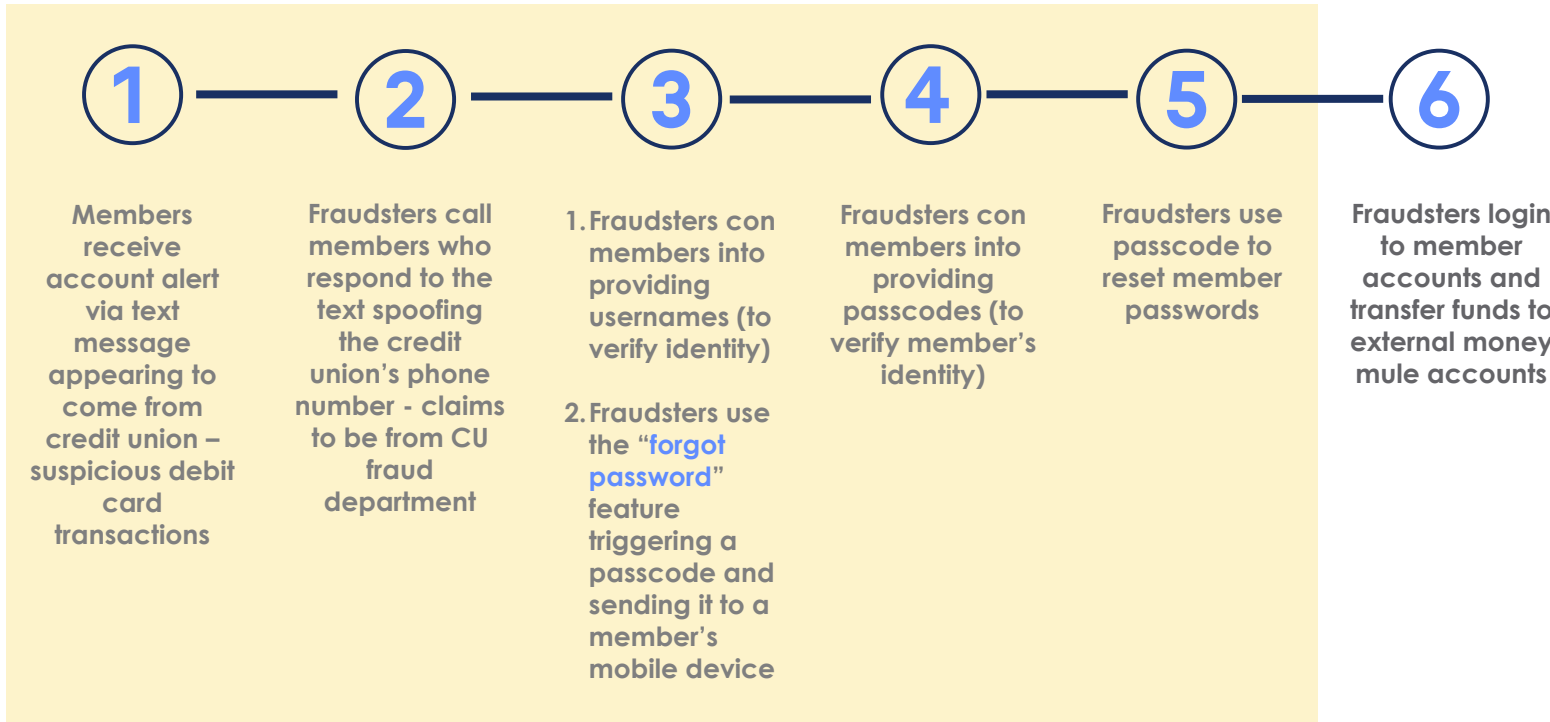
- Fraudsters recruit money mules to help launder proceeds derived from criminal activities
- May open fraudulent accounts using synthetic identities
- Adds layers of recipients to the money trail
- Complicates law enforcement's ability to trace money from a victim to criminal actor



Money mules & account takeovers

Account takeovers

Deploy tactics from the traditional Zelle fraud scam

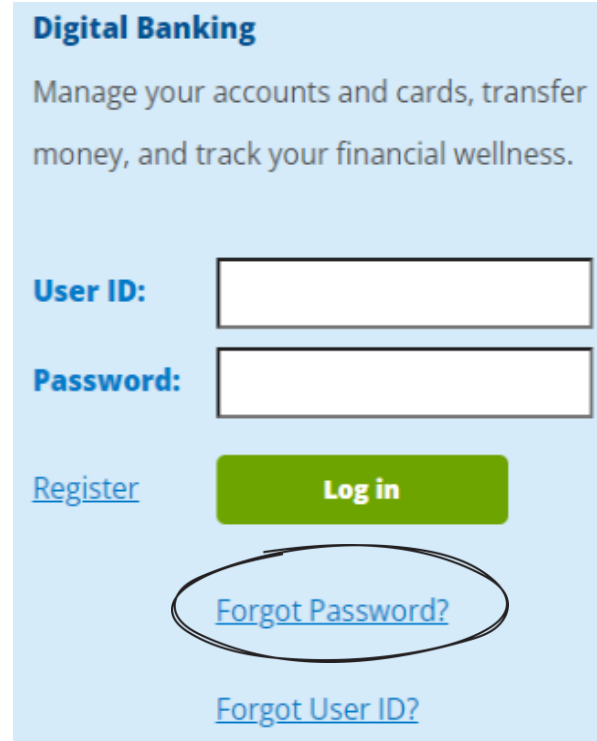


Variation of scam

- Text messages contain a link to spoofed website – CU online banking login
- Members click on the link and enter login credentials
- Fraudsters used credentials to immediately login to member accounts
- 2-factor authentication passcode delivered to members
- Members entered passcode to the spoofed site
- Fraudsters grab passcodes to complete login to member accounts
- Fraudsters transfer funds to external money mule accounts

\$2M account takeover fraud loss

- Members received a text alert appearing to come from the credit union – suspicious debit card transactions
- Members responding to the text received an immediate call from the fraudsters spoofing the credit union's phone number
- Fraudsters claimed to be from the credit union
- Fraudsters conned members into providing their online banking usernames – to verify their identities
- Fraudsters used the usernames with the “**forgot password**” feature – triggering a 2-factor authentication passcode to members
- Members conned into providing the passcode to the fraudsters – to verify their identities
- Fraudsters used the passcodes to reset members' passwords
- Logged into accounts and used A2A/external transfer service to transfer funds to external money mule accounts - \$2M in transfers in less than 2 weeks
- Credit union disabled A2A/external transfer service and the fraud stopped



Digital Banking
Manage your accounts and cards, transfer money, and track your financial wellness.

User ID:

Password:

[Register](#) [Log in](#)

[Forgot Password?](#)

[Forgot User ID?](#)

Account takeovers/money mules

- Account takeovers **and** money mule accounts at the same credit union
- Fraudsters recruit money mules to open fraudulent accounts at target credit union
- Social engineering attack launched against existing members to scam them out of their login credentials once the mule accounts are opened
- Fraudsters use member-to-member transfer feature to make large dollar transfers from compromised member accounts to the money mule accounts
- Money mules withdraw funds through various means

TruStage

RISK Alert

Actionable insights for bond policyholders

Awareness **Watch** Warning

Money mules & member-to-member transfers

Money mules are more prevalent in schemes orchestrated by fraudsters who seek to launder stolen funds obtained through account takeovers. Money mules are often recruited through social media platforms to open fraudulent accounts at specific credit unions, using their own identities as well as stolen and synthetic identities. Fraudsters promise the money mules they will make a lot of money. Money mules may open accounts online or in-person at a branch, in addition to using various methods to transfer funds. Most recently, the member-to-member transfer feature has been prevalent.

Alert details

Money mule activity is becoming more prevalent and the tactics they use highlights the complexity and sophistication of this financial scheme. A recent trend has the account takeovers and transfers to money mule accounts occurring at the same credit union. Some credit unions have experienced a significant number of account takeovers in a relatively short time resulting in large losses.

With account takeovers, fraudsters have typically transferred funds from compromised member accounts to external money mule accounts at other financial institutions.

Fraudsters posing as credit union employees continue to scam members into providing their online banking login credentials. Once logged into member accounts, the fraudsters use the member-to-member transfer feature to make large dollar transfers to recently opened money mule accounts. Some of the transfers to the money mule accounts were in the six-figure range.

Upon receiving the funds, the money mules withdraw the funds through various means, including in-person withdrawals at a branch, ATM, POS (usually to purchase gift cards), Cash App, Apple Cash and at casinos.

Fraudsters often recruit these money mules through social media; however, their approaches are always evolving. One credit union found a Facebook post soliciting individuals to open an account at the credit union for an opportunity to earn thousands of dollars.

Credit unions should remain cautious when opening new accounts due to the increase in this type of scheme. It underscores the importance of robust security tools and vigilance to protect members and the credit union.

Date: March 19, 2024

Risk category: Social engineering; fraud; scams; account takeovers; online/mobile banking; deposit account fraud

States: All

Share with:

- Branch operations
- Executive management
- Front-line staff/tellers
- Member services/new accounts
- Risk manager

Facing risk challenges?: **Schedule** a no-cost, personalized discussion with a Risk Consultant for more about managing risk.

\$2.5M account takeover fraud loss

- Fraudsters recruited money mules to open accounts at the credit union
- Fraudsters called existing members spoofing credit union's phone number claiming to be from credit union's fraud team
- Conned members into providing usernames that fraudsters used with the "forgot password" feature
 - Triggered 2FA passcodes to members – provided to fraudsters
 - Fraudsters used passcodes to reset passwords
- Fraudsters initiated member-to-member transfers to the mule accounts
- Money mules initially withdrew the funds in-person at branches but pivoted to electronic withdrawals

12/2023:
Fraud started

4/5/2024:
\$1.1M loss

5/22/2024:
Loss grew to \$2.5M



Money mules & fraudulent business accounts

Fraudulent business accounts

- Fraudsters recruit money mules to open fraudulent business accounts at credit unions to cash stolen checks, including U.S. Treasury checks
- Stolen checks were issued by a business and payable to another business
- Fraudulent accounts are opened in the name of the business listed as payee on the checks
- Fraudulent articles of incorporation filed with secretary of state
- Credit unions receive a breach of presentment warranty notice from drawee institutions claiming credit unions accepted check containing a forged endorsement
- For U.S. Treasury checks, credit unions receive a notice of reclamation – altered payee

Be on the lookout!

- The Secretary of State's filing stamp on articles of incorporation is dated a few days before the account is opened
- Stolen checks deposited to the fraudulent business accounts are dated 3-4 weeks before account was opened
- Payee's address listed on check bears no relationship to the address used to open the account
- Business name listed as payee on the check may not exactly match the name of the fraudulent business account

Fraud case study

Fraudulent business account

- Money mule opened a fraudulent business account at a credit union on 7/12/2023 to cash a \$549K stolen check
 - Account opened in the name of the payee on the check
 - Provided fraudulent registered articles of incorporation
- Funds withdrawn through various means after the check hold expired
- Credit union received a breach of presentment warranty claim from the bank on which the check was drawn
- Credit union impact: \$549K loss

Red flags

- Articles of Incorporation filed 11/19/2023
- Treasury check dated 8/29/2023
- Payee's address listed on Treasury check was NY (Queens)

Fraud case study

Fraudulent U.S. Treasury check

- Money mule opened fraudulent business account 11/27/2023 in the name of the payee (business) listed on stolen U.S. Treasury check
- Address used to open the account was VT
- Deposited stolen \$550k U.S. Treasury check on 1/4/2024 at a shared branch
- All funds were withdrawn by 6/4/2024 when the account was closed
- Notice of Reclamation received 11/22/2024

Red flags

- Payee's address listed on the check is Chicago, IL; whereas the account was opened using a Michigan address
- The check is dated one month (6/12/2023) before the account was opened
- Articles of incorporation filed on 6/26/2023

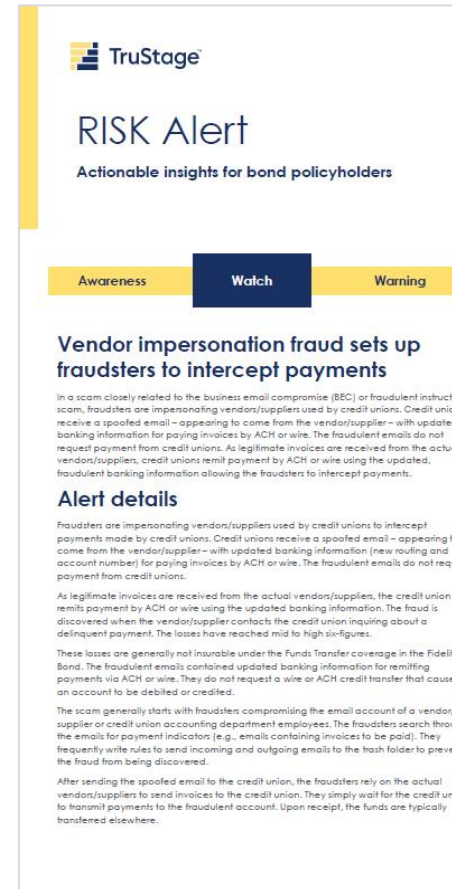


Can money mules increase litigation risks for credit unions?

Credit union sued to recover funds

Money mules may increase litigation risk and negatively impact your reputation

- Studco received fraudulent email appearing to come from Olympic Steel (a vendor used by Studco) containing updated banking instructions for remittances
- Studco followed the instructions and sent four ACH credit transfers totaling \$558k to CU for deposit to member/money mule's account
- Studco sued the credit union to recover the \$558k
- Incoming ACH credit transfers listed Olympic Steel as receiver – did not match name on member/money mule's account
- SEC code on the incoming ACH credit entries was "CCD" (corporate credit or debit) which is strictly reserved for commercial accounts



TruStage
RISK Alert
Actionable insights for bond policyholders

Awareness **Watch** Warning

Vendor impersonation fraud sets up fraudsters to intercept payments

In a scam closely related to the business email compromise (BEC) or fraudulent instruction scam, fraudsters are impersonating vendors/suppliers used by credit unions. Credit unions receive a spoofed email – appearing to come from the vendor/supplier – with updated banking information for paying invoices by ACH or wire. The fraudulent emails do not request payment from credit unions. As legitimate invoices are received from the actual vendors/suppliers, credit unions remit payment by ACH or wire using the updated, fraudulent banking information allowing the fraudsters to intercept payments.

Alert details

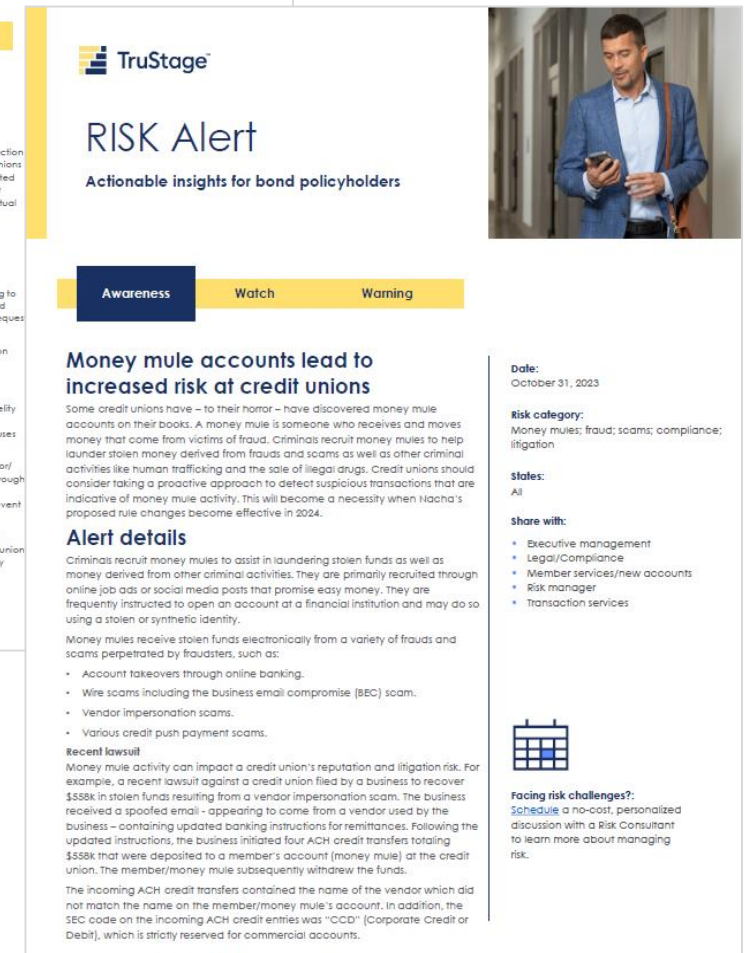
Fraudsters are impersonating vendors/suppliers used by credit unions to intercept payments made by credit unions. Credit unions receive a spoofed email – appearing to come from the vendor/supplier – with updated banking information (new routing and account number) for paying invoices by ACH or wire. The fraudulent emails do not request payment from credit unions.

As legitimate invoices are received from the actual vendors/suppliers, the credit union remits payment by ACH or wire using the updated banking information. The fraud is discovered when the vendor/supplier contacts the credit union inquiring about a delinquent payment. The losses have reached mid to high six-figures.

These losses are generally not insurable under the Funds Transfer coverage in the Fidelity Bond. The fraudulent emails contained updated banking information for remitting payments via ACH or wire. They do not request a wire or ACH credit transfer that causes an account to be debited or credited.

The scam generally starts with fraudsters compromising the email account of a vendor/supplier or credit union accounting department employees. The fraudsters search through the emails for payment indicators (e.g., emails containing invoices to be paid). They frequently write rules to send incoming and outgoing emails to the trash folder to prevent the fraud from being discovered.

After sending the spoofed email to the credit union, the fraudsters rely on the actual vendors/suppliers to send invoices to the credit union. They simply wait for the credit union to transmit payments to the fraudulent account. Upon receipt, the funds are typically transferred elsewhere.



TruStage
RISK Alert
Actionable insights for bond policyholders

Awareness **Watch** Warning

Money mule accounts lead to increased risk at credit unions

Some credit unions have – to their horror – have discovered money mule accounts on their books. A money mule is someone who receives and moves money that come from victims of fraud. Criminals recruit money mules to help launder stolen money derived from frauds and scams as well as other criminal activities like human trafficking and the sale of illegal drugs. Credit unions should consider taking a proactive approach to detect suspicious transactions that are indicative of money mule activity. This will become a necessity when Nacha's proposed rule changes become effective in 2024.

Alert details

Criminals recruit money mules to assist in laundering stolen funds as well as money derived from other criminal activities. They are primarily recruited through online job ads or social media posts that promise easy money. They are frequently instructed to open an account at a financial institution and may do so using a stolen or synthetic identity.

Money mules receive stolen funds electronically from a variety of frauds and scams perpetrated by fraudsters, such as:

- Account takeovers through online banking.
- Wire scams including the business email compromise (BEC) scam.
- Vendor impersonation scams.
- Various credit push payment scams.

Recent lawsuit

Money mule activity can impact a credit union's reputation and litigation risk. For example, a recent lawsuit against a credit union filed 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 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.

Date: October 31, 2023

Risk category:
Money mules; fraud; scams; compliance; litigation

States:
All

Share with:

- Executive management
- Legal/Compliance
- Member services/new accounts
- Risk manager
- Transaction services

Facing risk challenges?:
[Schedule](#) a no-cost, personalized discussion with a Risk Consultant to learn more about managing risk.



Lawsuit ruling

- Nacha rules and UCC 4A-207 (Misdescription of beneficiary) do not require RDFIs to match the receiver's name on incoming ACH credit entries to the name on the account
 - Under UCC 4A-207 if a CU notices a name mismatch, the ACH credit should be returned to avoid liability
- Credit union's system generated real-time alerts whenever a name mismatch was detected on incoming ACH transactions
 - Credit union did **not** review these alerts
- Credit union claimed to have no knowledge of the name mismatch
- Court ruled in favor of Studco
 - Court indicated that actual knowledge of the name mismatch can be imputed on credit union because real-time alerts were generated
- Credit union ordered to pay \$558k in compensatory damages

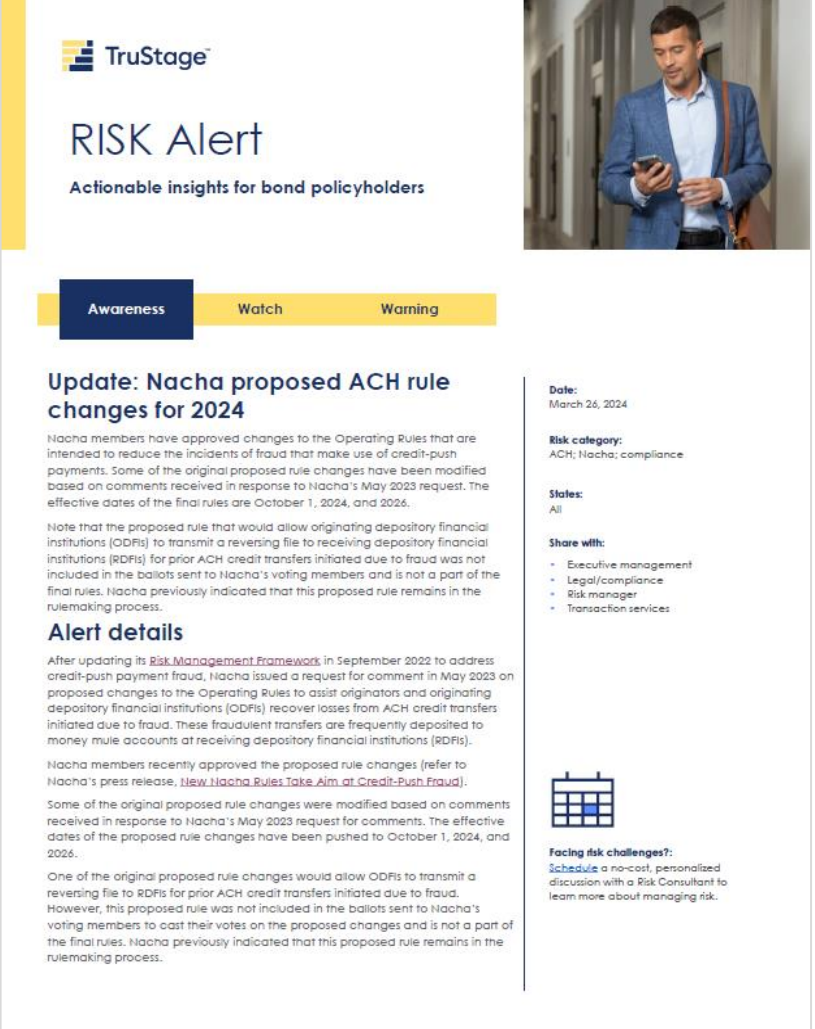




Nacha rule changes

Nacha rule changes

- Designed to assist originators and originating depository financial institutions (ODFIs) recover ACH credit transfers initiated due to fraud
 - Account takeovers
 - Fraudulently induced transfers
- Fraudulent ACH credit transfers frequently deposited to money mule accounts at receiving depository financial institutions (RDFIs)
- RDFIs will be required to establish risk-based procedures to identify incoming ACH credit transfers initiated due to fraud
 - Phase 1: RDFIs with annual ACH receipt volume of more than 10M in 2023 (effective date: 3/20/2026)
 - Phase 2: Applies to all RDFIs (effective date: 6/19/2026)



The graphic is a risk alert notification from TruStage. It features the TruStage logo at the top left. The main heading is 'RISK Alert' with the subtitle 'Actionable insights for bond policyholders'. Below this is a progress bar with three segments: 'Awareness' (dark blue), 'Watch' (yellow), and 'Warning' (yellow). The main content area is titled 'Update: Nacha proposed ACH rule changes for 2024'. It includes a date of March 26, 2024, and a risk category of 'ACH; Nacha; compliance'. The alert is shared with 'Executive management', 'Legal/compliance', 'Risk manager', and 'Transaction services'. A 'Facing risk challenges?' section suggests scheduling a discussion with a Risk Consultant. A small calendar icon is also present.

TruStage

RISK Alert

Actionable insights for bond policyholders

Awareness Watch Warning

Update: Nacha proposed ACH rule changes for 2024

Nacha members have approved changes to the Operating Rules that are intended to reduce the incidents of fraud that make use of credit-push payments. Some of the original proposed rule changes have been modified based on comments received in response to Nacha's May 2023 request. The effective dates of the final rules are October 1, 2024, and 2026.

Note that the proposed rule that would allow originating depository financial institutions (ODFIs) to transmit a reversing file to receiving depository financial institutions (RDFIs) for prior ACH credit transfers initiated due to fraud was not included in the ballots sent to Nacha's voting members and is not a part of the final rules. Nacha previously indicated that this proposed rule remains in the rulemaking process.

Alert details

After updating its [Risk Management Framework](#) in September 2022 to address credit-push payment fraud, Nacha issued a request for comment in May 2023 on proposed changes to the Operating Rules to assist originators and originating depository financial institutions (ODFIs) recover losses from ACH credit transfers initiated due to fraud. These fraudulent transfers are frequently deposited to money mule accounts at receiving depository financial institutions (RDFIs).

Nacha members recently approved the proposed rule changes (refer to Nacha's press release, [New Nacha Rules Take Aim at Credit-Push Fraud](#)).

Some of the original proposed rule changes were modified based on comments received in response to Nacha's May 2023 request for comments. The effective dates of the proposed rule changes have been pushed to October 1, 2024, and 2026.

One of the original proposed rule changes would allow ODFIs to transmit a reversing file to RDFIs for prior ACH credit transfers initiated due to fraud. However, this proposed rule was not included in the ballots sent to Nacha's voting members to cast their votes on the proposed changes and is not a part of the final rules. Nacha previously indicated that this proposed rule remains in the rulemaking process.

Date:
March 26, 2024

Risk category:
ACH; Nacha; compliance

States:
All

Share with:

- Executive management
- Legal/compliance
- Risk manager
- Transaction services

Facing risk challenges?
[Schedule](#) a no-cost, personalized discussion with a Risk Consultant to learn more about managing risk.

Summary of Nacha's new rules

- ODFIs, business originators and certain 3rd parties must implement risk-based processes to identify ACH credit entries initiated due to fraud (phased effective dates in 2026)
- RDFIs must implement risk-based processes to identify incoming ACH credit entries initiated due to fraud (phased effective dates in 2026)
- Expands the use of return reason code R17 for RDFIs to return an ACH credit entry believed to be initiated due to fraud (effective date 10/1/2024)
- Expands ODFIs ability to request RDFIs to return an ACH credit entry for any reason (effective date 10/1/2024) - RDFIs are not obligated to return the funds
- Provides RDFIs the option to delay funds availability from an incoming ACH credit transfer suspected as fraud (effective date 10/1/2024) – RDFIs must still comply with Reg CC's funds availability rules
- Establishes a new standard company entry description (PAYROLL) for PPD (prearranged payment and deposit) for payment of wages/salaries (effective date 3/20/2026)
- Establishes a new standard company entry description (PURCHASE) for e-commerce purchases (effective date 3/20/2026)
- The timing of the written statement of unauthorized debit (WSUD) would allow the receiver to sign/date WSUD on or after the date the entry is presented to the receiver (effective date 10/1/2024)
- RDFIs must initiate the return of unauthorized ACH debits to a consumer's account by the opening of the sixth banking day following the completion of its review of the consumer/receiver's WSUD (effective date 10/1/2024)

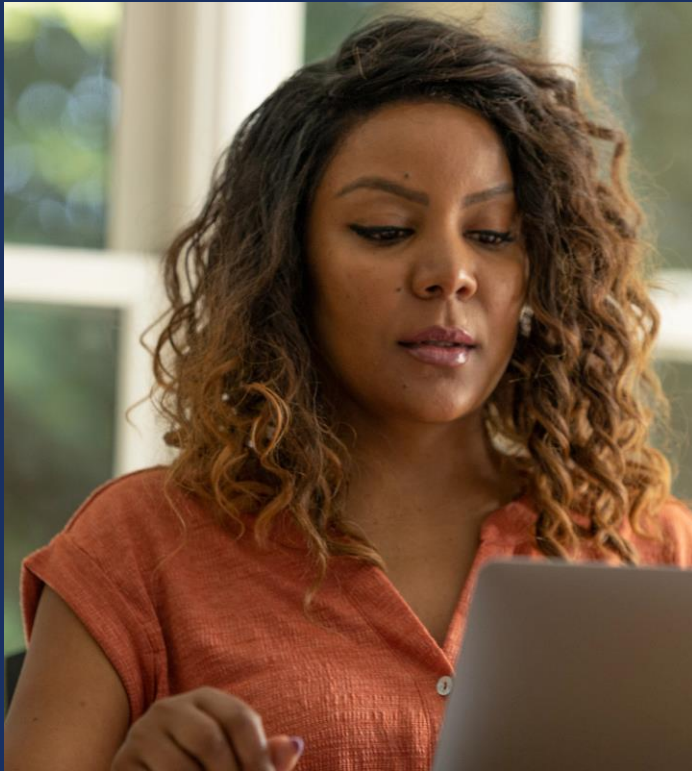


Money mule red flags

Money mule red flags

- Changes in transactional patterns for existing members
- Large dollar incoming transfers (ACH and wires) to new consumer/member accounts followed by immediate transfers out of the account
- Large dollar incoming wire transfers: Beneficiary's name contained in the incoming wire does not match the name on the member's account.
- Large dollar incoming ACH credit transfers: Receiver/member's name contained in the ACH entry does not match the name on the member's account
- 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)
- 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 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
 - The payee's address listed on the check bears no relationship to the address used to open the account

Risk mitigation strategies

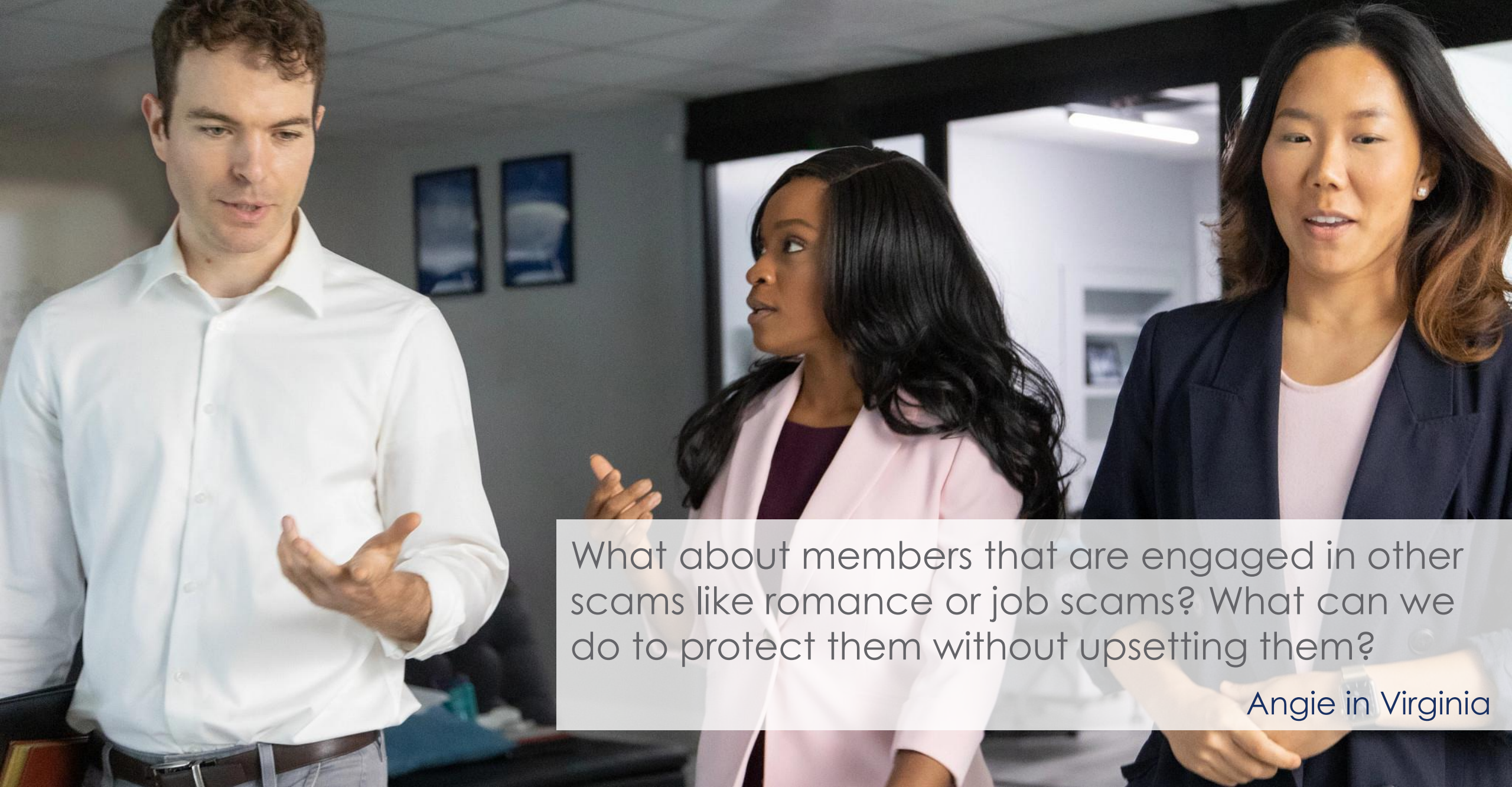


- Warn/educate members on how fraudsters recruit money mules and the role they play in money laundering
- Train staff on the role money mules play in laundering ill-gotten money along with the red flags that may be indicative of money mule activity
- Deploy an identity verification solution that can 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
- Generate a system alert whenever a name mismatch is detected in incoming ACH credit transfers and wires and the member's account
 - Return ACH credit entry (R17) or wire when a name mismatch is detected
- Generate an alert for mismatched commercial SEC codes on incoming ACH credit transfers to consumer accounts
 - CCD (Corporate Credit or Debit) and CIE (Consumer Initiated Entry) SEC codes are intended for commercial accounts – not consumer accounts
- Scrutinize new business accounts
 - Be alert for articles of incorporation that are filed shortly before the account is opened
 - Place extended holds on checks deposited to new business accounts

Don't forget about compliance

- BSA/AML laws require credit unions to monitor accounts for suspicious activity
- File a SAR when you detect suspicious activity that may be indicative of a money mule account





What about members that are engaged in other scams like romance or job scams? What can we do to protect them without upsetting them?

Angie in Virginia



- Most scams start with fake profiles on online dating, job, or other social media sites created by stealing photos and text from real accounts or elsewhere.
- Scammers trick their victims into thinking they're someone they're not
- Once trust is established, the victim may be more easily convinced to send their sweetheart money, provide access to their financial accounts by sharing login credentials, and, in some cases, even launder funds for them

Scams impacting members

Assisting members

If you believe a member is being scammed, attempt to gather additional information by asking questions:

- Did you recently make a large withdrawal from your account?
- There appears to be a recent change to your account. Do you mind if I go over the change with you?
- We noticed an increase in the use of your debit card. Do you mind if we review the transactions to make sure they were all completed by you?
- We noticed an increase in the number of checks written on your account. Do you mind if we review the checks and transactions to make sure they were all written by you?
- Are you being asked to send money to someone that is pressuring you to think too quickly? How much do you know about this person?

If your member thinks they are being scammed, encourage them to report it to the FTC at www.ReportFraud.ftc.gov





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

NCUA rule on expelling members

- Credit unions generally limit EFT services for members who are "unwitting" money mules
- Credit unions can expel members who are "witting" and/or "complicit" money mules
- A member can be expelled "for cause" by a two-thirds vote of a quorum of the FCU's
- FCU must have adopted the related standard bylaw amendment
- FCU must provide a copy of Article 14 to Appendix A to §701, or the optional standard disclosure notice contained in Article 14

The NCUA defines "for cause" as:

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

Law enforcement efforts



Money Mules Fuel Fraud

What are money mules?

Money mules are people who receive and move money obtained from victims of fraud. Some money mules know they've been recruited to assist criminal activity, but others become money mules without realizing their activity is benefiting fraudsters.

How do people become money mules?

- Responding to a job advertisement or social media post that promises easy money for little effort.
- Helping someone they've met online (possibly on a dating website) or over the phone by agreeing to receive and transfer money.

Whether it is cash, packages, gift cards, or virtual currency, assisting money movement puts money in the pockets of criminals and could lead to serious consequences for you.

By knowing the signs of money mule activity, you can protect yourself and your community, and avoid assisting fraudsters.

Think twice about agreeing to help people move money!

- Don't open a bank account or move money at someone else's direction.
- Don't give someone access to your bank account or debit card.
- Don't allow money from people you don't know to be deposited into your account.
- Don't take a job that promises easy money and involves sending or receiving money or packages.
- Don't agree to receive or forward packages.
- Don't agree to purchase gift cards or virtual currency at someone's direction.

If you've acted as a money mule, it is never too late to stop!

- Stop communicating with the person giving you direction.
- Tell your financial institution and consider changing accounts.
- Report suspicious communications or activity to law enforcement.
- Protect yourself by learning about scams and money mule activity.

Money mules help international criminal networks steal money from senior citizens, businesses, and people just like you.

#DontBeAMule

For more information, visit

www.justice.gov/civil/consumer-protection-branch/money-mule-initiative



Image © Europol

- DOJ, FBI, US Postal Service Inspection Service and other federal law enforcement agencies launched annual money mule initiative to disrupt money mule network
- 2024: Federal law enforcement took action against 3,000 money mules
- Actions taken against money mules
 - Criminal prosecution against "complicit" money mules
 - Warning letters to "unwitting" money mules
- Launched outreach programs to raise awareness and educate consumers on how fraudsters recruit money mules

DOJ money mule initiative education flyer

Risk resources

Business Protection Resource Center
www.trustage.com/bprc

- RISK Alerts – warning | watch | awareness
- Loss prevention library
- risk overviews, checklists & whitepapers
- Emerging risks outlook
- Live webinars, risk forums & office hours
- On-demand learning & interactive training modules

“Great information, excellent format. Presenters were engaging and knowledgeable in their respective fields.”

Executive Vice President - \$3B credit union



Contact us

800.637.2676

- riskconsultant@trustage.com
- [Ask a risk manager interactive form](#)
- [Schedule a 1:1 risk consultation](#)
- [Report a risk or scam](#)



Thank you.

Contact

riskconsultant@trustage.com

800.637.2676

This presentation was created by the CUNA Mutual Group based on our experience in the credit union and insurance market. 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 presentation/publication, nor does it replace any provisions of any insurance policy or bond.

TruStage™ is the marketing name for TruStage Financial Group, Inc., its subsidiaries and affiliates. TruStage Insurance Products offered to financial institutions and their affiliates are underwritten by CUMIS Insurance Society, Inc. or CUMIS Specialty Insurance Company. Cyber policies are underwritten by Beazley Insurance Group or other nonaffiliated admitted carriers.

This summary is not a contract and no coverage is provided by this publication, nor does it replace any provisions of any insurance policy. Please read the actual policy for specific coverage, terms, conditions, and exclusions.