



**Risk & Compliance Solutions** | [RiskConsultant@trustage.com](mailto:RiskConsultant@trustage.com)

Emerging risks outlook

# Fraud trends





# Losses on the radar



While each credit union has its own unique risk footprint, these fraud risks and trends should be on your radar

- Account takeovers
- Interactive Teller Machine (ITM) fraud
- ATM/ITM jackpotting
- Fraudulent checks/deposits
  - Fraudulent checks clearing member accounts
  - Fraudulent business accounts
  - Fraudulent U.S. Treasury checks




# Account takeovers

# Account takeovers/money mules

## Account takeovers & 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



### RISK Alert

Actionable insights for bond policyholders

AwarenessWatchWarning

#### 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.





# Account takeovers

## Multiple 7-figure losses reported

### Social engineer members out of login credentials

Social engineer call center employees into resetting member passwords and changing member contact information

Enroll member accounts for online banking

- Enters member's personal information – name, account #, address, mail address, phone number including mobile #
- Hacks member email accounts to intercept online banking enrollment passcode needed to complete enrollment

Funds transferred to money mules



# 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







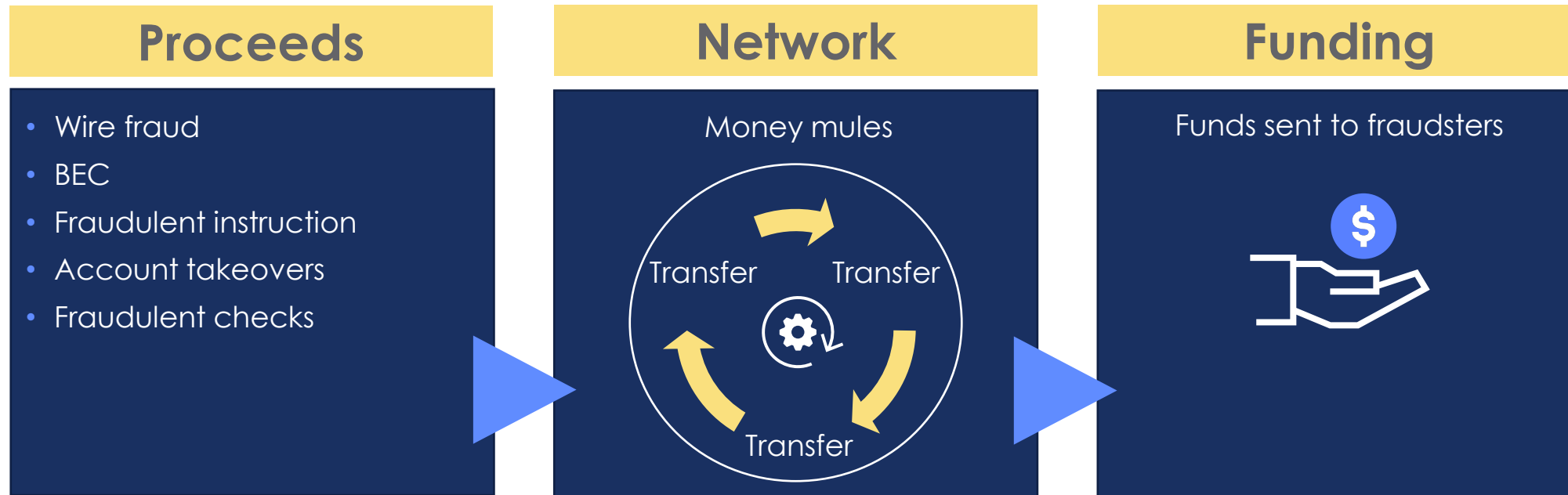
- **Social media outreach** with offers of easy money - fake job postings, direct messaging campaigns, and the creation of fraudulent business pages
- **Job advertisements** - fraudulent job listings with high salary offerings for minimal work, emphasizing remote work possibilities.
- **Phishing emails** 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?



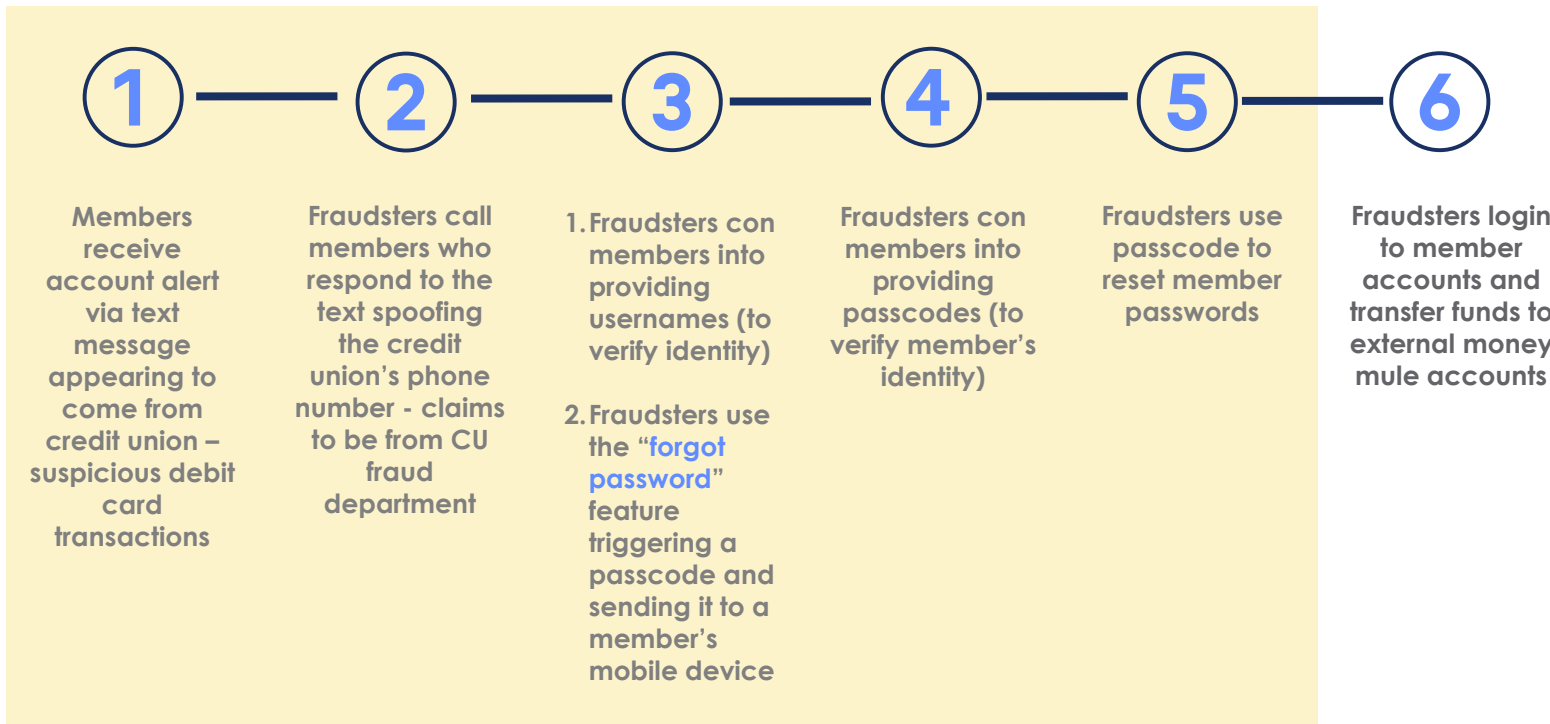
# Money mule role in laundering stolen funds



- 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

## Account takeovers

# Deploy tactics from the traditional Zelle fraud scam



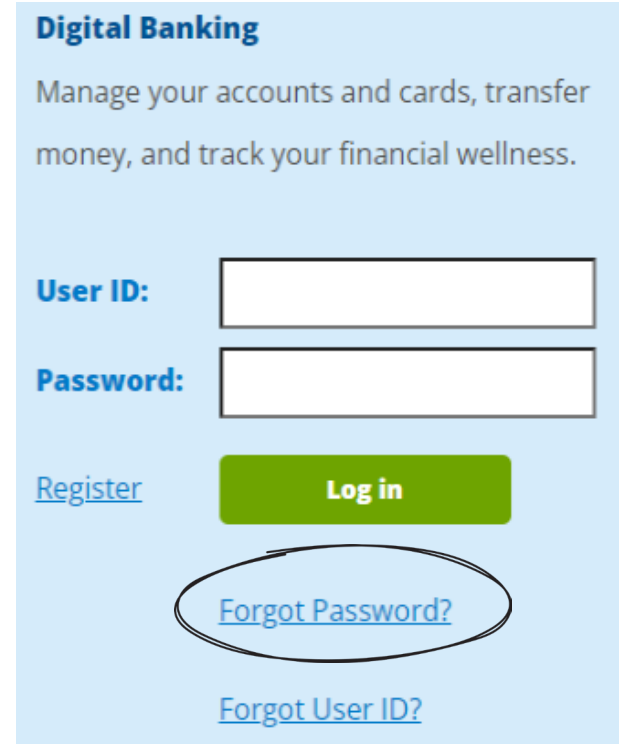
**Another variation of the scam** has fraudsters skip sending fraudulent text alerts and proceed directly to calling members spoofing the credit union's phone number to scam them out of their login credentials.

### 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?](#)



# \$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

# Change in tactics - \$500K account takeover fraud loss

## January 2025

- Fraudsters recruited money mules to open accounts at CU
- Launched social engineering attack to scam members into providing login credentials
- Used member-to-member (M2M) transfer feature to transfer funds out of the compromised member accounts to the mule accounts
- Money mules withdrew funds through various means
- Fraud stopped after CU wrote rule to prevent M2M transfers to new accounts for the first 30 days of account opening

## March 2025

- Fraudsters ramped up social engineering attacks against members
- Pivoted to using external transfer service to transfer funds out of the compromised member accounts to external money mule accounts
- Fraud stopped when CU disabled the external transfer feature
- CU will enable external transfer feature once Plaid is deployed

## March – April 2025

- Fraudsters pivoted to using bill pay to issue checks to money mules
- CU is looking into disabling bill pay's check feature but may start by lowering the limit for bill pay checks

# Account takeovers & Reg E protection

## Reg E's definition of an unauthorized EFT [§1005.2(m)]

"Unauthorized electronic fund transfer" means an electronic fund transfer from a consumer's account **initiated by a person other than the consumer** without actual authority to initiate the transfer and from which the consumer receives no benefit.

## Additional clarification in the commentary to §1005.2(m)

3. Access device obtained through robbery or fraud. An unauthorized EFT includes a transfer initiated by a person **who obtained the access device from the consumer through fraud or robbery.**

## CFPB's EFT FAQs

The CFPB's Electronic Fund Transfers FAQs clearly indicate that members victimized in this scam are entitled to Reg E protection and should be recredited.

**Members victimized in the traditional scam are entitled to Reg E protection.**

Refer to the CFPB's Electronic Fund Transfers FAQs:  
<https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/>



## Account takeover

# Online wire fraud - \$800,000 loss impact

- Credit union offered online wires through online banking (consumer platform)
- Online wire requests processed by a credit union employee
- Fraudster impersonated a member and social engineered call center employees
  - Reset member's online banking password
  - Changed member's contact information (home & mobile phone numbers; email address)
- Fraudster logged into account
  - 2FA triggered but passcode delivered to fraudster via text message
  - Requested 2 wires totaling \$800k
- Callback verifications were performed but calls went to the fraudster who answered security questions

**Note: Wires are governed by Article 4A of the Uniform Commercial Code (UCC 4A)**



## Account takeover

# Online wire fraud - \$400,000 loss impact

- Fraudster social engineered call center employee into resetting member's online banking password
- Fraudster social engineered mobile phone carrier call center employee into porting member's mobile service to the carrier using the same phone number
- Fraudster logged into member's account and requested a \$400K wire by completing an online wire form
  - 2FA triggered a passcode via text message – received by the fraudster
- Wire processed by a credit union employee
- Callback verification performed using the mobile phone number on the member's account
- Fraudster received the call and answered security questions

**Note: Wires are governed by Article 4A of the Uniform Commercial Code (UCC 4A)**



# Risk mitigation strategies



- Properly authenticate members enrolling for online banking through CU's website – avoid sending online banking enrollment passcodes via email due to email hacking risk
- Don't allow members to use the "forgot password" feature using an unregistered device
- Deploy a more secure form of 2-factor authentication – such as a token or push notifications to a dedicated app on members' device
- Deploy a real-time fraud monitoring solution with behavioral analytics that leverages AI and machine learning (e.g., DataVisor)
- Set reasonable monetary limits, including member-to-member transfers
- Avoid resetting passwords based on a member's phone request

## Important fraud rules

- Block/review P2P, wires and external transfers that are initiated immediately following a password reset
- Block/review large-dollar member-to-member transfers to new accounts OR create rule to prevent M2M transfers to new accounts for the first 30-60 days of account opening



# Bond condition 12 & loss mitigation

- Credit unions may find themselves in the midst of an account takeover scam incurring thousands of dollars in daily fraud losses
- Condition 12 requires credit unions to take all reasonable measures to minimize the loss
- Educational campaigns warning members of the scam are ineffective
- Step ladder approach to deploying loss controls
- Controls aren't working? Disable the payment type targeted by fraudsters to transfer funds out of the compromised member accounts to money mules
  - Account-to-account (A2A)/external transfer service
  - Zelle/P2P
  - Member-to-member transfers
- Failure to mitigate the loss could jeopardize a claim



## Discovery of loss

### Risk overview



As an insured of the TruStage™ Fidelity Bond, your organization is required to follow certain conditions and responsibilities – including taking all reasonable measures to minimize the loss after it is discovered. The failure to effectively mitigate a loss after it is discovered could impact whether the loss is afforded coverage.

### Key conditions

As an insured of the TruStage Fidelity Bond, your organization is required to follow these important conditions:

#### Condition 10 - Discovery of loss

Discovery of a loss occurs "when your officer, branch manager, risk manager or director first becomes aware of facts which would cause a reasonable person to assume that a loss of a type covered under this Bond has been or will be incurred," regardless of when the loss occurred.

#### Condition 11 - Notice of discovery of loss

Notice of discovery of loss requires credit unions to send written notice of Discovery Of Loss to TruStage as early as practical, but not to exceed 90 days after such discovery.

#### Condition 12 - Your duties after discovery of loss

Your duties after discovery of loss requires credit unions to submit a complete, sworn proof of loss which "must include the necessary explanation and documentation to prove the cause of the loss, the amount of the loss and the identity of the persons, if known, who caused the loss." Condition 12 also requires credit unions to "take all reasonable measures to minimize the loss" once it is discovered.

### Reasonable measures to take to minimize the loss

#### Scenario 1:

##### Fraudulent checks clearing a member's checking account

A member reports multiple fraudulent checks clearing their credit union checking account. Reasonable measures to mitigate the loss could include the following:

- Closing the account and issuing a new account number with new checks to prevent future occurrences by the same wrongdoers.
- Attempting to return the fraudulent checks unpaid by the midnight deadline to the depository institution where they were deposited.
- Requesting the depository institution to return the funds if the midnight deadline has passed.
- Pursuing a breach of presentment warranty claim under UCC 4-208 (Presentment warranties) against depository institutions that accept an altered check or a check containing a forged endorsement that is drawn on a member's account.



# Interactive teller machine (ITM) fraud

# ITM fraud – unauthorized withdrawals from member accounts

## What's happening?

- Fraudsters target the self-service feature at outside ITMs during non-business hours (late night over weekends)
- Access member accounts using counterfeit debit cards at ITMs
- Many found deep insert skimmers on their machines
- Others had fraudsters access member accounts using an alternate authentication allowed by the ITM – such as a combination of account number plus a SSN or date of birth
- In some cases, fraudsters took advances against member home-equity line-of-credit (HELOC) loans at the ITMs
- Mid six- and seven-figure losses are common





# ITM fraud risk mitigation

## In general

- Block all fallback transactions at ITMs and ATMs
- Set reasonable daily withdrawal limits
- Use skimming/shimming detection technology
- Conduct daily inspections of all ITMs/ATMs – including opening to inspect for deep shimmers
  - If foreign device or tampering is detected – machine should automatically shut down
- Ensure all ITMs and ATMs are EMV-enabled
- Educate members of risk at ITM/ATMs – report any signs of tampering

## ITM self-service option:

- If a debit card is used to authenticate members, ensure ITM reads the EMV chip, if it is not detected decline the transaction
  - Do not allow fallback transactions
- Avoid using easily compromised identification to access accounts (i.e.: SSN, DOB, account number)
  - Implement one-time passcodes sent to member devices before proceeding with transaction access
- Set reasonable daily withdrawal limits
  - Single transaction and daily limits
- Do not allow access to line of credit accounts
- Limit hours of operations to normal business hours for self-service option and require members to use video teller if available. Machines can function as ATM during nonbusiness hours

# ITM fraud case studies

## Credit union A

- **Date of loss:** March 24, 2023
- **Members affected:** 197
- **Total loss:** \$1,747,785
- **Loss per member:** \$8,872
- Withdrawals occurred over a 4-hour period using the self-service feature
- Multiple individual member losses over \$50,000

## Credit union B

- **Date of loss:** March 4, 2024
- **Members affected:** 302
- **Total loss:** \$393,990
- **Loss per member:** \$1,305
- Withdrawals occurred over a 6-hour period using the self-service feature



### The disparity in losses:

- Both credit unions had a single withdrawal limit of \$2,500 but Credit Union A did not have a daily limit – fraudsters made multiple \$2,500 withdrawals from a single member's account
- Credit Union A allowed members to take advances against line-of-credit loans (e.g., HELOCs) using the self-service feature while Credit Union B did not
- Credit Union A: Fraudsters took advances against member HELOCs to fund the withdrawals



# ITM/ATM jackpotting

# ITM/ATM jackpotting – causes machine to dispense cash

## What's happening?

- Most common: fraudster **infects the machine with malware**. Usually by inserting a flash drive containing malware into the USB port – simply by accessing the ATM/ITM top hat
- Fraudsters connect a **black box**, usually a laptop, directly to the ATM dispenser to send commands to the machine to disburse cash until its empty
- **Man-in-the-middle attack**. Fraudsters install a device between the ATM's computer and the network cable connection to the acquirer's host system. Requires the fraudsters to insert any card - like a gift card or a stolen card – and messages are intercepted and modified

## Mitigation tips

- Work with ATM/ITM vendor
- Replace the ATM/ITM top hat lock and equipping it with an alarm is critical - use an audible alarm to startle the criminal and get them to flee
- Encrypt the machine's hard drive
- Encrypt the communication between the machine and the acquirer's host system. If a router is used, the communication link between the machine and the router must also be protected.
- Ensure the ATM/ITM operating system is supported and ensure security patches are installed when they're made available
- Dispense throttling – shuts down machine when velocity of cash dispensed reaches a specified limit
- Frequent inspections



# Fraudulent checks/deposits



# Fraudulent checks/deposits



- Significant increase in both frequency and severity of losses
- Deploying tactics from well-known scams
- Money mules continue to assist
- Stolen mail is a key driver



- Steal members' issued checks and alters them or manufactures fraudulent checks using info from legitimate checks
- Recruit money mules to open accounts at credit unions to cash stolen checks, including Treasury checks
- Open fraudulent business accounts in the name of the payees listed on stolen checks



# Fraudulent checks clearing member accounts

## What's happening?

- Fraudsters steal members' issued checks from blue drop boxes
- Alter checks (payee) and dollar amount
- Manufacture fraudulent checks using the information from members' legitimate checks

- Credit unions can recover losses from members' altered checks (as well as checks containing a forged endorsement)
  - Pursue a breach of presentment warranty claim under UCC 4-208 against depository institutions that accept members' altered checks
- Credit unions typically take the loss from fraudulent checks created using information from members' legitimate checks
  - Checks must be returned by the credit union's midnight deadline
- Ensure members report unauthorized checks within the specified time frame in account agreement

# UCC 4-208 presentment warranties



When a depository institution accepts a check for deposit or payment it makes certain warranties to the drawee institution under UCC 4-208:

- The depository institution is entitled to enforce the check (i.e., check does not contain a forged endorsement)
- The check has not been altered
- The depository institution has no knowledge that the drawer's (account holder) signature is unauthorized
- For remotely created checks, the person on whose account the item is drawn authorized the issuance of the item in the amount for which it is drawn

**Note:** Credit unions must pursue the breach of presentment warranty claim within 30 days of learning of the breach. Missing the deadline does not absolve the depository institution of its liability; however, the credit union may not be able to recover the full amount.

# Breach of Presentment Warranty Claim under UCC 4-208

- For checks drawn on the credit union
- Send written demand to depository institution
- Depository institution breached a presentment warranty under UCC 4-208 by accepting an altered check or one containing a forged endorsement
- Include a copy of the item (front and back)
- Include affidavit of alteration (if altered check) or affidavit of forged endorsement
  - Use the correct affidavit
- The date of affidavit may be viewed as the date of discovery so send the demand letter within 30 days of the date of the affidavit

Pursuing a breach of warranty claim under UCC 4-208 >>> [Risk overview & sample letter](#)

## Appendix 2 Sample presentment warranty claim letter

Date

Name of Depository Institution  
Address of Depository Institution

To whom it may concern:

This letter constitutes our claim against your institution arising from your institution's breach of a presentment warranty under the Uniform Commercial Code (UCC) § 4-208, Presentment Warranties. Your institution accepted the following check(s) drawn on our credit union (we are the paying institution):

Drawer Name	Date of Check	Check Number	Payee Name	Dollar Amount
			Original Payee: Altered Payee:	Original Amount: Altered Amount:
			Original Payee: Altered Payee:	Original Amount: Altered Amount:

Type of Presentment Warranty Claim:

- ☐ Altered Item  
☐ Forged Endorsement  
☐ Missing Endorsement

We are making this claim under UCC § 4-208, Presentment Warranties: UCC § 4-208 provides that the depository institution warrants to the institutions in the forward collection process and ultimately the paying institution that:

- The depository institution is entitled to enforce the check (i.e., the check does not contain a forged endorsement or missing endorsement), and
- The check has not been altered

Description of our claim:

Please direct any questions to:

Name, Title:  
Credit Union Name:  
Phone Number:  
Email Address:

Please forward payment in the amount of \$\_\_\_\_\_ at your earliest convenience to:

Name, Title:  
Credit Union Name:  
Street Address:  
City, State Zip Code:

Enclosures:

- Check copies (enter #)
- Affidavit of forgery
- Affidavit of alteration



## Some FIs are denying credit union breach of presentment warranty claims

- They're wrong
- Be persistent – make 2nd & 3rd requests
- Threaten legal action, if necessary
- These financial institutions will eventually return the funds to the credit union

1. Pursuant to UCC § 4-208, the check is counterfeit/washed/traced or was not otherwise signed by an authorized signer of the drawer. The signature of the client on this check is not similar to the signature on other items we have pulled drawn by the maker, your customer. You, as the paying bank, had a responsibility to verify the signature. Because the signature is questionable, we decline to pay the claim.

# When fraudulent checks clear a member's account

- Open new account with new account number and freeze old account
    - Request list of outstanding checks from member
    - Manually clear the checks against the old account as they're presented for payment
  - Determine if the member reported the unauthorized checks within the timeframe outlined in the account agreement
    - Don't recredit member if reported late
  - If applicable, pursue a breach of presentment warranty claim against the depository institution
- Perform manual review of large dollar checks (e.g., \$10,000 or more) presented for payment
    - Verify member signatures against reliable specimens (e.g., signature card or loan documents)
    - Call member to verify that they actually issued the check to the stated payee for the amount listed
      - Check the member's account to make sure the phone number was not changed in the last 60 days before making the call
    - Review must be performed timely to allow the credit union to return unauthorized checks by their midnight deadline
  - Consider offering payee positive pay to business members

# Benefits of offering payee positive pay to business members

- Credit unions must recredit members for unauthorized checks clearing their account provided the member reports them within the time frame specified in the account agreement
- Offering payee positive pay to business members can significantly reduce the credit union's risk of loss
- Credit unions may be able to shift liability for unauthorized checks to business members that refuse payee positive pay (refer to [Cincinnati Insurance vs. Wachovia Bank](#))
  - Business account agreement must contain liability shifting disclosure language
  - Work with legal counsel to develop liability shifting disclosure language
- Several large banks' business account agreements shift liability for unauthorized checks to businesses who refuse payee positive pay service
  - Wells Fargo, Bank of America and TD Bank



# Fraudulent business accounts



# Fraudulent business accounts

## What's happening?

- Fraudsters - or their money mules - open fraudulent business accounts to cash stolen checks, including Treasury checks, that are made payable to a business
- Account opened in the name of the business listed as payee on the stolen check
- Fraudsters file fraudulent articles of incorporation with the secretary of state and provide this document to the credit union at account opening
- Credit unions receive a breach of presentment warranty claim from drawee institutions claiming credit unions accepted check containing a forged endorsement
- For Treasury checks, credit unions receive a notice of reclamation – forged endorsement

## Red flags

- Articles of incorporation dated just days before the fraudulent business account is opened
- Stolen checks are dated 3 to 8 weeks before the date of filing stamp on the articles of incorporation
- Payee's address on the check bears no relationship with the address used to open the fraudulent business account
- Business name listed as payee on the check may not exactly match the name of the fraudulent business account

## Fraudulent business account

# case study - \$549,000 loss impact

- 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 - filed 6/26/2023
- 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

### Red flags

- Articles of Incorporation filed 6/26/2023
- The check was dated 6/12/2023
- Payee's address listed on the check was Chicago – account opened using a Michigan address



## Fraudulent U.S. Treasury check case study - \$550,000 loss impact

- Money mule opened fraudulent business account at a Vermont credit union on 11/27/2023 in the name of the payee (business) listed on stolen Treasury check dated 8/29/2023
- Address used to open the account was Vermont – payee's address listed on check was Queens, NY
- Deposited stolen \$550,000 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 was Queens, New York
- The check is dated three months (8/29/2023) before the account was opened
- Articles of incorporation filed on 11/19/2023



# Risk mitigation – fraudulent business account



- Deploy identity verification solution to verify the identity of new members
- Verify business entities by obtaining registered articles of incorporation
  - Be wary of recently filed articles of incorporation
- Do a search on the business name
- Place extended holds on checks deposited to new accounts in accordance with Reg CC
- Exercise caution when new members present large dollar checks, including U.S. Treasury checks, for deposit or payment
  - Consider accepting the checks for deposit to member savings accounts so that a longer hold (e.g., 11 days) can be imposed (subject to state laws in CA, CT, MA and NY)
- Consider establishing a waiting period before new members can use remote deposit capture service





# Risk mitigation for Treasury checks

- Verify security features on U.S. Treasury checks
  - Using a black light helps
- Verify Treasury checks using the Treasury Check Verification System (TCVS) - <https://tcvs.fiscal.treasury.gov/>
  - Recent enhancement allows credit unions to verify payees
  - Only available via the API version
  - Must complete the Terms and Conditions document
- Verify IRS Treasury checks using the U.S. Treasury Inspector General for Tax Administration (TIGTA) Check Integrity system
  - <https://tigta.app.box.com/f/3387a408f287465fbef62493329794db>



#### Wrap-up

- Stay on top of the changing fraud environment
- Craft risk mitigation strategies accordingly
- Rinse & repeat – it's a continuous process



# Risk resources

## Business Protection Resource Center [www.trustage.com/bprc](http://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

**TruStage**

### RISK Alert

Actionable insights for bond policyholders

**Awareness** **Watch** **Warning**

#### Fraudulent business accounts opened to cash stolen checks

Fraudsters are opening fraudulent business accounts of credit unions to cash stolen checks that were issued by businesses to other businesses. It is believed the stolen checks are a result of the stolen mail problem occurring in a growing number of states.

The fraudulent accounts are opened in the name of the business, or a similar name, and listed as the payee on the stolen checks. The credit unions reported receiving breach of presentment warranty claims under UCC 4-208 from drawers institutions to reimburse the institutions for accepting a check containing a forged endorsement.

**Alert details**

Stolen mail has resulted in a significant increase in losses from fraudulent checks passing to members' accounts. Another by-product of the stolen mail problem has fraudsters opening fraudulent business accounts of credit unions to deposit stolen checks. The stolen checks are issued by businesses and made payable to other businesses. The fraudsters open fraudulent business accounts using the payee's name and deposit the stolen checks. The funds are subsequently

**Date:**  
November 4, 2024  
(previously issued: April 25, 2023)

**Risk category:**  
Fraud; Business accounts; Scams; New account fraud; Check fraud; Deposit account fraud; Compliance

**States:**  
All

**Share with:**

- Accounting
- Branch operations
- Executive management
- Front-line staff
- Legal/compliance
- Member services/New accounts
- Risk manager
- Transaction services

**TruStage**

### Fraudulent U.S. Treasury Checks

**Risk overview**

A significant increase in fraudulent U.S. Treasury checks has occurred over the last few years. Fraudsters manufacture counterfeit Treasury checks as well as steal issued Treasury checks out of the mail. They then recruit money mules to open fraudulent accounts at credit unions, including fraudulent business accounts, to cash the fraudulent Treasury checks. The losses can be significant ranging from five-figure to high six-figure amounts.

Fraudsters manufacture counterfeit Treasury checks as well as steal issued Treasury checks out of the mail. They then typically recruit money mules to open fraudulent accounts at credit unions, including fraudulent business accounts, to cash the fraudulent Treasury checks.

Money mules open accounts of credit unions in person at a branch as well as online through the credit union's website. In most cases, the money mules open the accounts using their own identity, but they can also open the account using a synthetic or stolen identity.

The fraudsters or money mules also open fraudulent business accounts to cash stolen Treasury checks that are made payable to a business. They open the account in the name of the business listed as payee on the stolen checks. Alternatively, the fraudsters alter the payee listed on the check replacing it with another business name. The fraudsters file fraudulent articles of incorporation with the secretary of state and provide this document to the credit union at account opening.

The fraudulent Treasury checks are returned through the Federal Reserve as "altered/forged." However, in many cases, credit unions received a reclamation notice from the U.S. Treasury due to the payee being altered or the payee's endorsement was forged or unauthorized.

The U.S. Treasury's Bureau of Fiscal Service implemented a new payee name validation capability within the [Treasury Check Verification System](#) (TCVS) Application Programming Interface (API). Payee name validation is only available through the API. Refer to Federal Reserve's [New payee name validation ability for Treasury Check Verification System](#). The U.S. Treasury Inspector General for Tax Administration (IGTA) also has a program where financial institutions can request verification of suspicious IRS Treasury checks.

**Red flags that may signal new account fraud**

- The secretary of state's filing stamp on the articles of incorporation is dated just days before the fraudulent business account is opened. In some cases, the filing stamp is dated the day before the account is opened.
- The stolen Treasury checks are dated 4 to 5 weeks before the date of the secretary of state's filing stamp on the articles of incorporation.
- In many cases, the payee's address on the check bears no relationship with the address used to open the fraudulent business account. For example, the payee's address listed on the check is in Georgia; however, the address used to open the fraudulent business account is in Michigan.

**TruStage**

Risk & Compliance Solutions | Presentation

## Emerging risks outlook

Rethinking protection in an era of uncertainty

Proprietary and confidential. Do not distribute.

0:00:00



# Thank you.

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.