



Risk & Compliance Solutions | Risk forum

Transactions & fraud

Don't fall victim

Proprietary and confidential. Do not distribute.



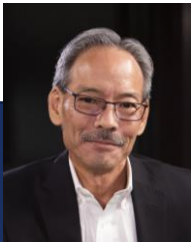
Today's session



Becky Garton
Risk Consultant - Wisconsin



Holly Spiczenski
Risk Consultant - Wisconsin



Ken Otsuka
Risk Consultant - Illinois



David Spielbauer
Senior Claims Manager



What's on tap?



- Transactions & fraud trends
- Focused risk topics
- Your questions

Fraud & scams on the radar



- ACH debit fraud & account takeovers
 - Stolen mail & check fraud
 - Wire fraud
 - Fraudulent business accounts
 - P2P/Zelle fraud
 - Card not present fraud
- Business email compromise (BEC)
 - Fraudulent instruction – real estate
 - Ransomware
 - Social engineering fraud
 - Member scams
 - Elder abuse & exploitation fraud

What's trending

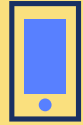
- P2P/Zelle fraud
- Junk fees
- Account takeovers & new account fraud
- ACH debit fraud
- ChatGPT



Spoofer website & Zelle

\$690,000 loss impact

- Fraudsters launched widespread SMiShing campaign
- Members received text alerts appearing to come from credit union
- Text messages contained link to a spoofed website – credit union's online banking login page
- Members clicked on the link and entered their login credentials
- Fraudsters used credentials to immediately login to member accounts
- 2-factor authentication passcodes delivered to members
- Members entered passcodes on the spoofed website
- Fraudsters grabbed passcodes to complete login to member accounts
- Used Zelle to transfer funds to others



- ABC CU: Unusual activity on 4/1, \$500 at Getcoins. If this wasn't you, visit <https://abccuonline.org> to dispute
- ABC CU: Unusual activity on 4/4, \$599.99 at Walmart. If this wasn't you, visit <https://abccuonline.org> to dispute
- ABC CU ALERT: Your account is temporarily suspended due to suspicious activity. Please visit <https://abccuonline.org> to reactivate your account

Risk mitigation strategies

- Introduce Zelle with lower daily limits (limits can be raised later)
- Require members to enroll for Zelle in person at a branch or through call center after they are properly authenticated (active enrollment)
- Don't allow password resets using unregistered devices
- Block/delay Zelle transfers that occur immediately following a password reset
- Consider a rule for a lower limit for new tokens
- Deploy real-time fraud monitoring system
- Include a statement in texts and emails containing 2-factor authentication passcodes: If you did not request this passcode, call the credit union immediately. Don't share this passcode with anyone. Credit union employees will never ask for this passcode.
- Disable Zelle during the midst of the fraud
- Conduct member education



P2P/Zelle fraud & 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.

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/>

Focus on consumer protection



CFPB has placed significant focus on “junk fees” and overdraft fees.

- Cited institutions for the unfair practice of assessing APSN overdraft fees on debit card transactions
- Cited institutions for unfair practice of assessing multiple NSF fees on the same transactions (NSF fees charged on represented/resubmitted items that are returned unpaid)
- It is uncertain whether disclosing the mechanics of a debit card transaction, including APSN overdraft fee practices and multiple NSF fees for resubmitted transactions will mitigate litigation risk
- Review CFPB’s actions with legal counsel
- Make a business decision about whether to continue your APSN overdraft fee and multiple NSF fee practices on same transactions

Credit unions are offering ACH capabilities

- Account-to-account (A2A)/ external transfer service
- Online account opening – funding via ACH
- Payments via ACH on credit cards and other loans
 - Online banking
 - Card processor's service (e.g., mycardinfo.com)
 - Pay-by-phone/online payment service
- Gift cards reloadable via ACH



ACH debit fraud

- Involves fraudulent new accounts and account takeovers
- Fraudulent new accounts opened online mainly at credit unions with an association or charitable organization within the field of membership (FOM)
- May be funded with fraudulent ACH deposits (ACH debits)
- Fraudsters immediately enroll for online banking once the account is opened
- Use external transfer service to pull funds from external accounts (ACH debits) for deposit to newly opened account
- Funds transferred elsewhere before the ACH debit entries are returned unpaid



Online account opening & funding

- Deploy identity verification solution
- Ensure ACH funding limit is reasonable
- Compare geolocation of IP address used to open account to new member's address
- Avoid using the automated approval feature – particularly over weekends and for new members who qualify by joining the association or by making contribution to charitable organization within FOM
 - These applications should be manually reviewed
- Consider screening high-risk applications through a more robust identity verification solution – such as a skip tracing solution
- Send welcome package to new members



Risk mitigation for external transfer service

- Conduct due diligence on members to qualify them for this service due to the risk associated with originating ACH debits
- Implement a reasonable daily monetary limit. The monetary limits should include a rolling 30-day limit
- Consider tiered limits
 - A tier with lower limits for new members/new users
 - A tier with higher limits for established members / established users
- Consider placing a hold on funds deposited via ACH debit (deposits via ACH debit are exempt from Regulation CC's funds availability rules)
- Although not foolproof, use trial deposits to validate the ownership of the funding account
- Consider a vendor's account validation solution
(Refer to [**Nacha's Account Validation Resource Center**](#) for a list of preferred partners)

Risk mitigation for account takeovers

- Properly authenticate members who enroll for online banking through CU website
- Deploy a secure form of out-of-band/2-factor authentication, such as a token
- Deploy real-time fraud monitoring solution with behavioral analytics
- Don't allow members to use the "forgot password" feature using unregistered devices
- Avoid resetting online banking passwords based on a telephone request





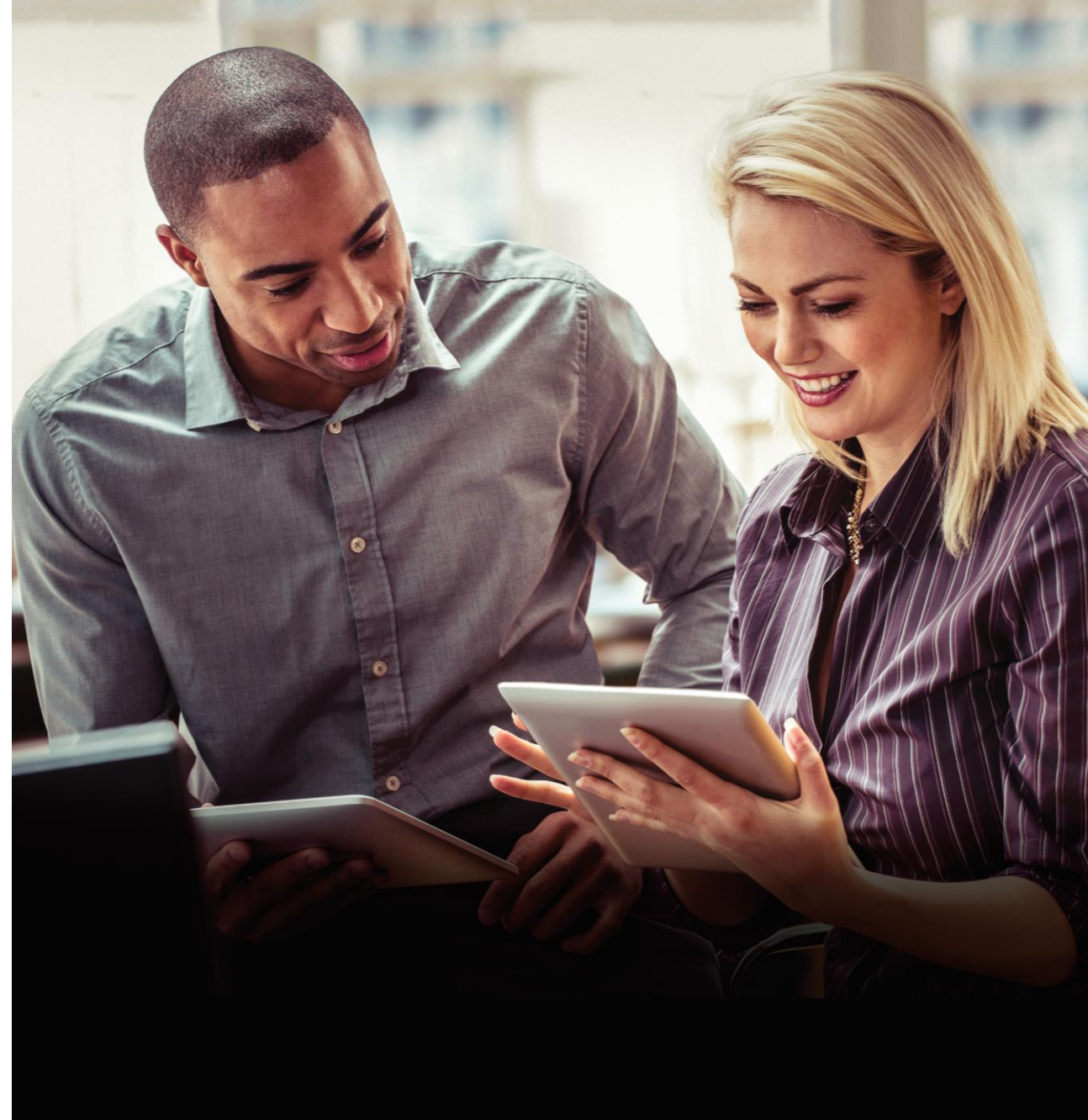
ChatGPT can make it difficult to distinguish between AI and human-crafted messages.

Chatbots easily craft convincing scam emails without the common mistakes non-native English speakers tend to leave in their copy.

Attackers can also leverage ChatGPT for in-depth learning about target organizations.

ChatGPT biggest risks

- **Generation of phishing emails** - it can produce well-crafted phishing emails in multiple languages without common warning signs
- **Creation of malware** - due to its ability to generate code in many languages, it can create malware to detect sensitive user data, hack entire computer systems, or scan email accounts
- **Privacy issues** – it retains the user's sensitive info, which can pose a data threat if it gets misused
- **Inaccurate data or missing information** - ChatGPT is trained on vast amounts of data, and in the case of inaccurate data or missing information, the responses will reflect those issues
- **Biased content** – answers have been provided that are not aligned with cultural diversity
- **Plagiarism** – text can be generated that is similar to existing content based on training data patterns.



Tips to limit risks if using ChatGPT

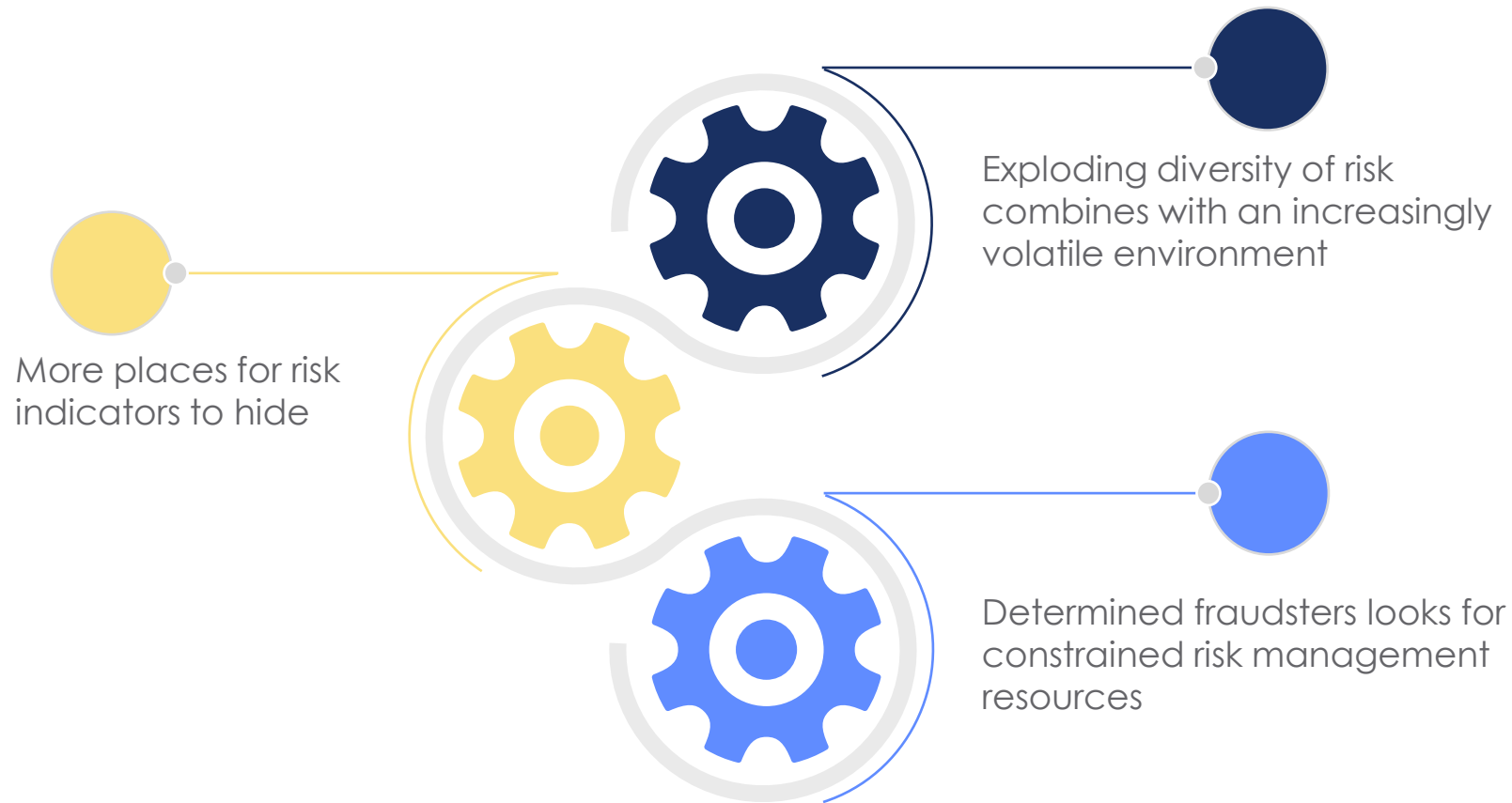


- Do not share any personal information and sensitive data with ChatGPT. You can send an email to OpenAI and request to delete your data, in case you or one of your employees already shared it.
- Carefully analyze and verify the content of any suspicious emails and do not click on any link.
- Have a difficult-to-guess password.
- Install effective anti-virus software and have a two-factor authentication process.
- To protect your system from cyberattacks, keep your software updated with the latest security installations as outdated software can put your business at risk.

Do not take any legal, medical, or financial advice from ChatGPT

Transaction & fraud risks are evolving

Effective risk management and need for strategy is even more critical



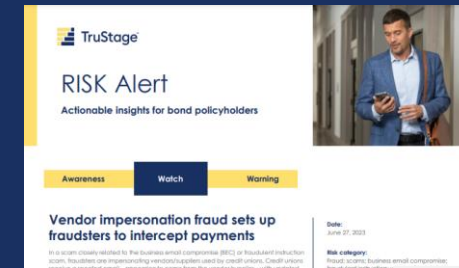
Business Protection Resource Center

Business Protection Resource Center (BPRC) www.trustage.com/bprc

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

“Great webinars - serious, important information delivered in a relaxed, ‘we’re among friends’ way.”

\$9B credit union





Session deep-dive:

③ risk hot topics

Check fraud/stolen mail

‘What’s going on’ insights from a claim perspective



David Spielbauer
Senior Claims Manager



Down...but not out

Over the past 20 years, check usage has declined by nearly two-thirds

3.4B

of checks written by
Americans in 2022 according
to Federal Reserve

680k

reports of check fraud by
financial institutions to FinCEN
in 2022

300k

reports of mail theft by the
U.S. Postal Inspection Service
in 2021

Consumers write nearly 75% of checks with 40% involving a payment to a business. Often sent via the mail.

Old scheme, new twist



- Fraudsters are:
 - targeting USPS blue drop boxes
 - robbing postal workers to steal their universal drop box key
 - 412 postal workers in 2022 & 305 so far in 2023 robbed of their keys
 - 38,500 thefts in 2022 + 25,000 this year from mail receptacles

Source: [United States Postal Service, May 12, 2023](#)

Typically, after last pick up of the day or on Sundays/holidays when there is no pickup, fraudsters break into the blue boxes and steal any mail inside

The result is a treasure trove of PII along with legitimately issued checks

- The PII can be used to steal member identities and perform account takeovers
- Stolen checks give fraudsters ability to alter the check or create their own fraudulent checks using the same MICR information

Common coverages for check fraud

Fraudulent Deposit

Member negotiates a fraudulent check through their account and causes a loss

Unauthorized Signature

Fraudster signs/endorsees a check with their own name, instead of your member's name, and you relied on that endorsement in paying the item

Forgery or Alteration

Check is stolen from mail and the payee/amount is washed

Counterfeit Share Draft, Checks or Securities

Fraudsters gain access to member account and create fraudulent checks that imitate legitimate drafts drawn on the account

Common issues for covered check fraud

Fraudulent Deposit

- Requires the member intended to deceive/defraud the credit union in the deposit
- Often requires the member be the actual person to make the deposit
- Requires the member knew the item would not be paid

Unauthorized Signature

- Requires you have on record the signatures of all authorized users on the account
- Requires the credit union relied on the signature in paying the item



Common issues for covered check fraud

Forgery or Alteration

- Forgery must be the reproduction of another natural person's signature
- Member cannot benefit from the item/transaction

Counterfeit Share Draft, Check Or Securities

- Requires there be an original item that is being imitated



Risk mitigation



- Close account and issue new account number
- If applicable, pursue breach of presentment warranty claim against depository institution
- Determine if member reported the unauthorized checks within the timeframe outlined in account agreement
- Perform manual review of large dollar checks (e.g., \$25,000 or more) presented for payment
 - Verify member signatures against reliable specimen (e.g., signature card or loan documents)
 - Verify check characteristics against member's legitimate check
 - Call member to verify that they issued the check to the stated payee for the amount listed. Verify the phone number on the member's account was not changed in the last 60 days prior to 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

Encourage members:

- Pay bills online or use the bill paying service.
- Mail checks inside the Post Office lobby rather than using blue mailboxes.
- Log into accounts frequently to review transaction history – looking for unfamiliar transactions.
- Report unfamiliar & unauthorized transactions immediately to the 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](#)

Business email compromise, fraudulent instruction & website spoofing

Fraud focused on the ease of providing quick instruction



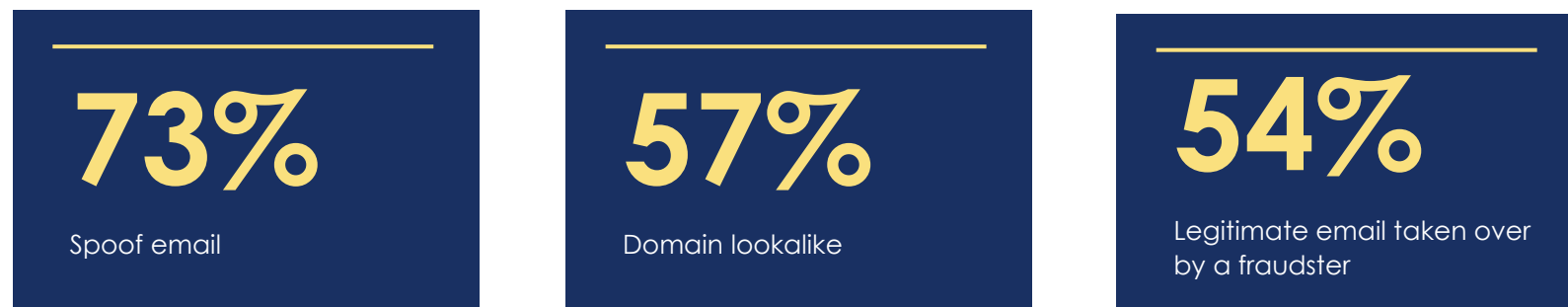
Holly Spiczenski
Risk Consultant - Wisconsin



Most prevalent types of BEC fraud

\$2.7B adjusted loss for BEC crimes against businesses & consumers

Source: Source: IC3's 2022 Internet Crime Report, FBI



Source: 2022 ITRC Annual Data Breach Report, IDTheftCenter.org

71% of organizations experienced attempted or actual BEC in 2022.

Source: Source: 2023 Payments Fraud and Control Survey Report, Association for Financial Professionals

Business email compromise

- A fraudster compromises the CEO's email and then sends a well-crafted email to another member of the c-suite or employee with instructions to complete a transaction.
- The recipient complies with the email message and authorizes the payment or information release often without following appropriate follow-up protocols.
- The money or data is then wired to or shared with the fraudster as the instructions requested.



Actual BEC loss scenarios

Case of the investment purchase

- Credit union CEO's email hacked. Fraudster found email exchanges with CFO
- Fraudster created rule to send all incoming and outgoing emails to the trash folder
- Fraudster sent email to CFO from within the CEO's email account requesting a \$500,000 wire to purchase investment while CEO was out of office
- Fraudster sent another email to the CFO the next day (from within the hacked account) requesting a \$1.5 million wire
- Second wire didn't go through as CEO confirmed she didn't send the email

Case of the remodel invoice

- Credit union was remodeling a location
- CEO's email was hacked, and fraudster found email exchanges with contractor
- Fraudster sent spoofed emails to accounting department to pay invoices via wire transfer
- Initial loss was nearly \$10 million; however, credit union was able to recover \$7 million

Source: Internal Claims Data, CUMIS Insurance Society, Inc.

BEC/fraudulent instruction red flags

- Sense of urgency
- Requests typically come from a high-level executive or authority
- Often coincide with being out-of-the-office
- Requests to keep transaction confidential and only communicate through email
- Often coincide with changes in direct deposit information or for payments to be made to a different account
- May impersonate a trusted supplier, vendor or business partner
- Misspellings, poor grammar and emails sent outside of normal business hours

From: CEO@acmecorp.com
To: Jane@acmecorp.com
SUBJECT: Urgent

I need you to initiate a wire transfer in the sum of \$45,250 to the account below. I am boarding a flight, and this needs to be done right now. Can you please get this done?

Send confirmation of the transfer immediately only to this email.

Thanks



ChatGPT can make it difficult to distinguish between real and fraudulent messages

Fraudulent instruction

- Fraudulent instruction wire scams typically involve a fraudster looking to trick a member, credit union employee, or even a title company or closing agent
- Usually conducted via email with fraudulent instructions to wire funds to the fraudster at the last minute for a real estate transaction
- Last-minute instructions within spoofed emails
- Common email subject lines:
 - Wiring instructions have been updated
 - We have sent you the wrong wiring instructions



Actual fraudulent instruction loss scenarios

Member loss of \$187,000

- The member is purchasing a new house with sufficient funds on deposit at the credit union.
- The title company's email is hacked, and the fraudster locates this loan closing information.
- The fraudster sends a spoofed email to the member with last minute, updated wire instructions which are bogus.
- The member followed the updated instructions and requested the wire in person at a branch location.
- The member's funds were no longer available at the closing.

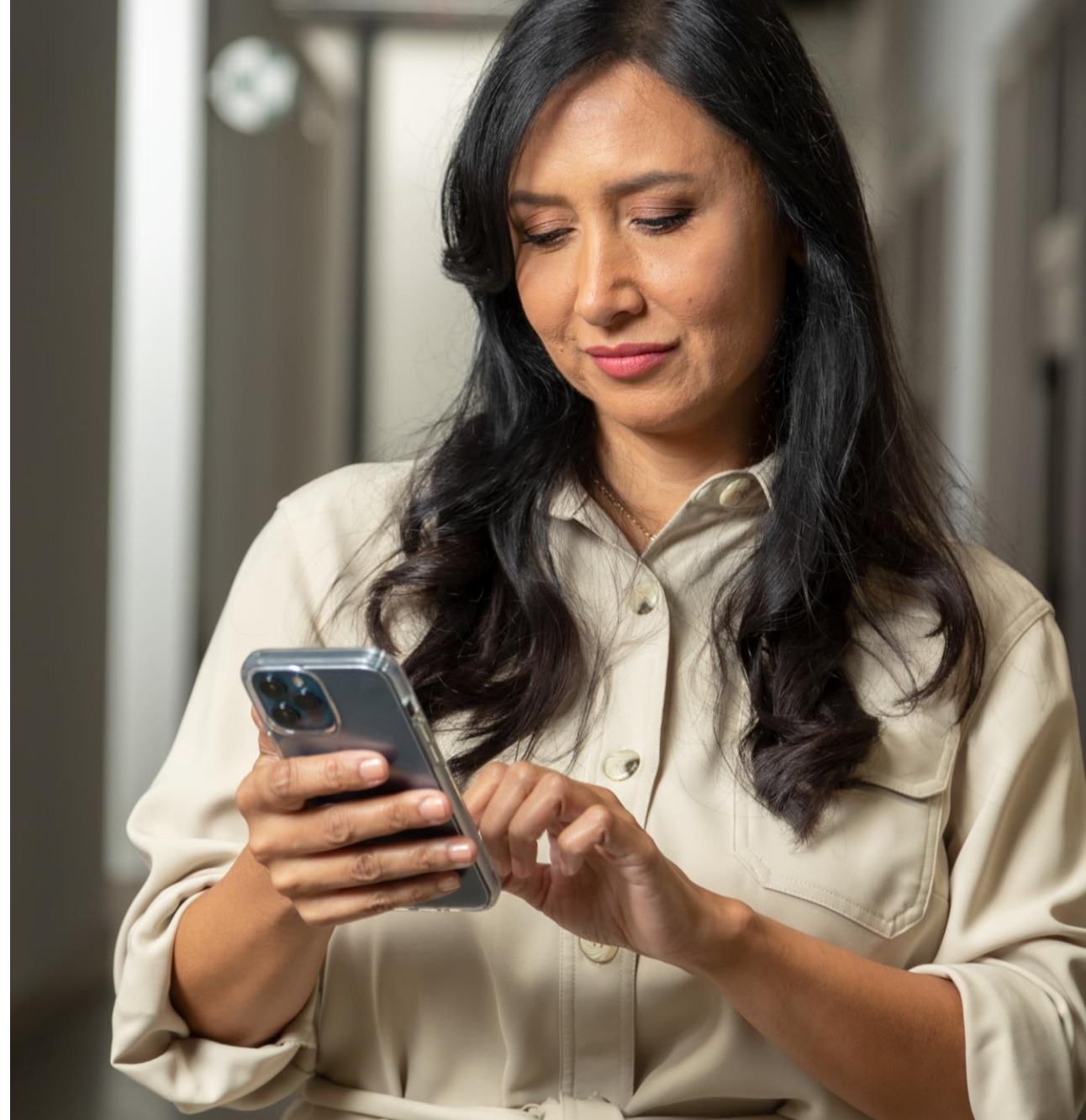
Credit union loss of \$1.7M

- The credit union mortgage department employee's work email is unknowingly hacked.
- The fraudster finds email exchanges between the employee & the title company president.
- The fraudster spoofs the title company president's email and sends an email to employee with updated wire instructions for all future closings.
- The updated instructions were bogus and impacted three members' closings.

Source: Internal Claims Data, CUMIS Insurance Society, Inc.

Mitigation tips

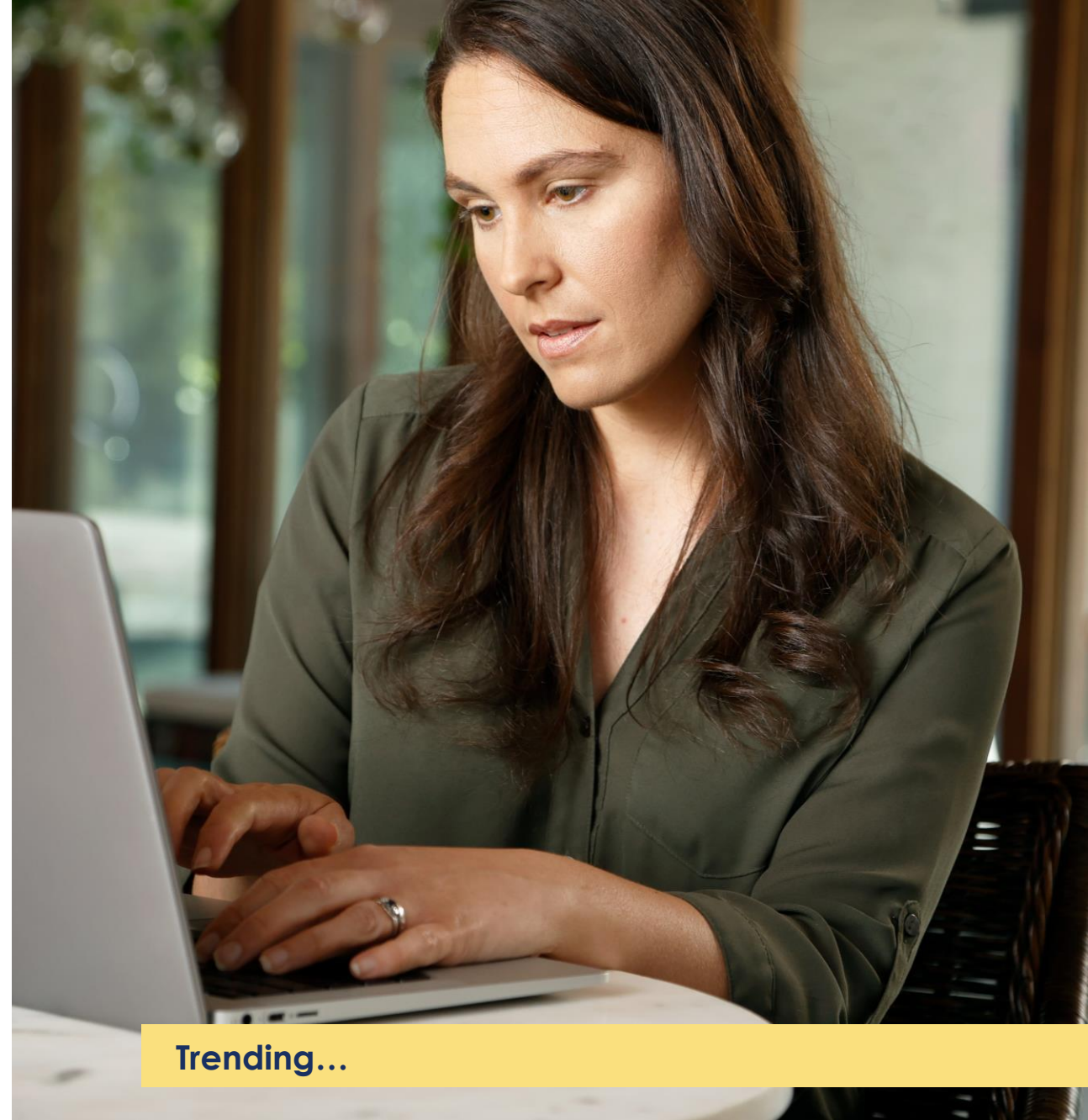
- Confirm the legitimacy of the request by verifying with the c-suite executive
- Authenticate using a different communications channel (out-of-band authentication)
 - Verify face-to-face with the requestor
 - Call the requestor's phone extension or cell phone
- Implement dual controls for handling internal wire transfer requests or payments
- Add EXTERNAL warning in subject line for incoming emails originating outside of credit union
- Add email banner warning the employee
- Verify "updated wire instructions" via callback using reliable phone number



Fraudulent instruction for vendor remittance

- Fraudsters impersonate legitimate vendors/suppliers used by credit unions
- Credit union receives a spoofed email appearing to come from their vendor/supplier with updated banking information (new routing # & account #) for paying invoices
- The fraudulent emails do not request a funds transfer
- As legitimate invoices are received from the actual vendor/supplier, the credit union remits payment via ACH or wire using the updated banking information
- Discovered when credit union received delinquency notices from the vendor/supplier

Generally, not insurable under funds transfer coverage as a funds transfer is not requested – only updated information for remitting payment



Trending...

Text messages & spoofed websites

Fraudulent text messages - appearing to come from the credit union – containing links to spoofed websites are being sent to members

- Member's account has been locked or suspended due to suspicious or fraudulent transactions
- Unusual/suspicious transactions at Walmart
- Unusual/suspicious transactions at cryptocurrency exchanges
- Suspicious Zelle transfer

Members are instructed to click on the link which takes the members to spoofed credit union websites where they are instructed to enter their login credentials – usernames and passwords.

The fraudsters immediately use the credentials to login to the member's accounts, make changes, and remove funds.



Trending...

RISK Alerts

Business Protection Resource Center www.trustage.com/bprc

- Warning | watch | awareness
- Just-in-time email distribution
- Accessible within the Business Protection Resource Center & as a PDF
- Recommended routing list
- Risk mitigation tips
- Related resource links

19,000+ subscribers

RISK Alerts Library

[Loss Prevention Library](#)
[RISK Alerts library](#)
[Webinars and education](#)
[Contact us](#)

Search

Select a Risk

Search

Clear

Title/Date	Risk	Summary	Recommended Resources
ATM Skimming & Fuel Theft Transactions Back to the Store 6/16/2022	ATM	ATMs are once again an easy target for fraudsters to capture card data - and, again, it is through skimming/grepping devices found on credit union-owned ATMs. Since the implementation of EMV/Chip cards, these devices have occasionally gone undetected leading to a large number of cards being compromised. The cards are used at other ATMs or through POS transactions where fraudsters rely on failed transactions to override the EMV safeguard to obtain cash and/or merchandise.	<ul style="list-style-type: none"> ATM Skimming Checklist ATM Safeguards
Laboratory Services Back to the Store 6/16/2022	ATM	Many municipalities have been against encumbrance and siting on public property. As a result, it takes people to provide commercial properties for credit unions and ATM enclosures, laboratories and accessories.	<ul style="list-style-type: none"> Member Services Checklist ATM Safeguards

[Tools & resources](#)
[Claims support documents](#)
[Business Protection Support Center](#)
[Forms/applications search](#)
[Frequently asked questions](#)
[RISK Alerts library](#)

RISK Alert

Actionable insights for bond policyholders

Awareness

Watch

Warning

Text messages & spoofed websites used to lure members into scam

Fraudulent text messages - appearing to come from the credit union - containing links to spoofed websites are being sent to members. The spoofed websites are made to look like the credit union's legitimate websites and members are enticed to click on the link and share confidential information such as username, password, as well as 2-factor authentication passcodes. These fraud attempts have resulted in losses from account takeovers.

Alert details

Sending third text message phishing is quickly becoming a preferred choice of fraudsters to lure members into giving up their credentials or sensitive information. There have been multiple reports of members receiving fraudulent text messages containing links to spoofed websites made to look like the credit union's legitimate site.

The text messages have the following themes:

- Member's account has been locked or suspended due to suspicious or fraudulent transactions.
- Unusual/suspicious transactions at Walmart.
- Unusual/suspicious transactions at cryptocurrency exchanges.
- Suspicious bank transfer.

Members are instructed to click on the link contained in the message which takes the members to spoofed credit union websites where they are instructed to enter their login credentials - username and password. The fraudsters immediately use the credentials to login to the member's accounts.

Once the fraudsters used unregistered devices to login to the accounts, a 2-factor authentication passcode is generated and delivered to the member who, in turn, enters the passcode on the spoofed website. The fraudsters immediately use the passcodes to complete the login to the member accounts.

Once logged into the member's accounts, the fraudsters change the member's contact information and then remove funds using Zelle/PP or ACH transfer.

In other instances, the fraudster calls or texts the member in which they claim to be from the credit union and need the one-time passcode.

The primary institutions that have been used to move funds to have included Wells Fargo, Green Dot, Bancorp Bank, or Coastal Community Bank. However, there may be more financial institutions being used.

Date: June 20, 2023

Risk category: Fraud Scams (phishing; Funds transfer; Wire transfer; ACH fraud; Account takeover; Mobile banking)

States: All

Share with:

- Executive management
- IT
- Member services/new accounts
- Risk manager
- Transaction services
- Web development

RISK Alert

Actionable insights for bond policyholders

Awareness

Watch

Warning

Corporate check fraud reported 06/13/2023

These credit unions report their corporate check accounts are being fraudulently used:

- Front Royal Federal Credit Union, VA
- Cashen Federal Credit Union, TX
- Credit Union 1, NC
- Dugan Federal Credit Union, TX
- Seville Credit Union, MI
- First Federal Credit Union, MI
- Credit Union, MD

Details on the following pages of this Alert. For additional insights, fraud situations, please use the credit union contact information specific situation.

How to spot counterfeit checks and forgeries:

- ing/fraud to verify employees are complying with check hold policies and procedures.
- in process.
- check deposits in accordance with Regulation CC and the liability policy.
- account history and average balance to help identify unusual
- one checking account daily.

Action Resource Center: for additional mitigation tips and exclusive online training modules (User ID and Password required).

Date: June 16, 2023

Risk category: Scams; check fraud; corporate checks

States: All

Share with:

- Branch operations
- Front-line staff/tellers
- Member services
- Risk manager
- Teller supervisor
- Transaction services

Facing risk challenge?

Schedule: a non-credit, personalized discussion with a Risk Consultant to learn more about managing risk.

TruStage®

Proprietary and confidential. Do not distribute.

38

Real-time payments

The speed of instant payments compounds fraud challenges



Ken Otsuka
Risk Consultant - Illinois

Real-time payments



- To be classified as real-time (or instant) payment, the payment option must:
 - enable both payer and payee to immediately see the transaction reflected in their respective account balances, and
 - provide funds that the payee can use immediately after the payer initiates the payment
- Real-time payments, by its nature, are irrevocable (i.e., cannot be reversed by the payer or payer's financial institution)
- Payments must settle instantaneously between the payee's financial institution and payer's financial institution
- Receive only role versus send and receive role
- **Real-time payment networks:**
 - The Clearing House's RTP Network®
 - FedNow_{SM} Instant Payments
 - Zelle

Don't confuse real-time payments with faster payments

Real-time payments are instantaneous

Faster payments, such as same-day ACH, are not instantaneous

Real-time settlement

- Real-time/instant settlement means that the transfer of final funds between the payer's and payee's financial institution occurs with the transmission of the payment message and just seconds before the payee's financial institution makes the funds available to the payee
- Payee's financial institution does not incur credit risk because it receives final funds from the payer immediately



Real-time payments

The players

- **End users** – consumers, businesses, nonprofits, government entities and others who want to take advantage instant payments
- **Financial institutions** – provide instant payment services to end-user customers
- **Interbank network operators** – organizations that operate the central clearing and/or settlement arrangements that enable participating financial institutions to complete real-time payment transactions

Types of transactions

- Peer to peer (P2P)
- Account-to-account (A2A) transfers - through the real-time payment network – not by ACH
- Bill pay
- Consumer to business (C2B)
- Business to consumer (B2C)
- Business to business (B2B)
- Consumer to government (C2G)
- Government to consumer (G2C)
- Business to government (B2G)

Risks of real-time payments

- Senders only
- No time to review transfers for potential fraud
- Real-time payments are irrevocable
- Account takeovers
- Scams targeting members –
 - Social engineer members into providing login credentials (think Zelle/P2P scam)
 - Authorized push payment scams
- New account fraud – opened by fraudsters or money mules to receive fraudulent payments



Controls for real-time payments

Online banking

- Properly authenticate members enrolling for online banking through credit union website
- Avoid sending online banking enrollment passcodes via email
- Deploy strong layered security controls
 - Real-time fraud monitoring solution
 - 2-factor authentication via token or push notifications
- Adopt reasonable transaction limits – daily, weekly and monthly

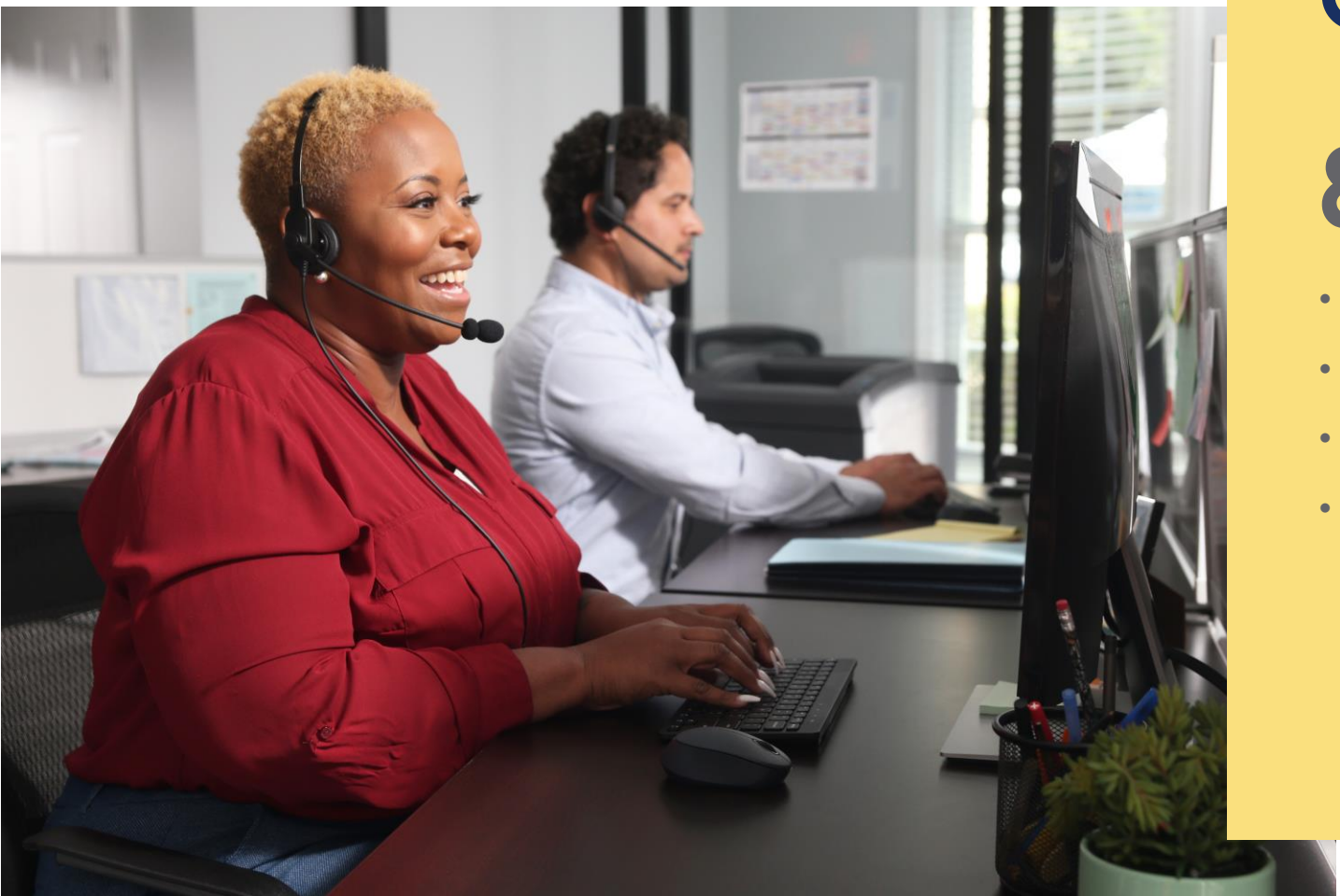
Fraudsters often defeat/intercept 2FA sending passcodes via automated phone call, SMS text, and email

- Hack member email accounts
- Social engineer credit union call centers to change a member's contact information (e.g., mobile phone number)
- Social engineer members
- Social engineer mobile carriers – SIM swap scam and port-out scam
- Mobile malware that redirects calls and text messages to fraudsters



Other controls

- Don't allow members to use "forgot password" feature using unregistered devices
- Avoid resetting passwords based on phone requests
- In the absence of an identity verification solution in the call center, avoid accepting phone requests for real-time payments
- Member education



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](#)

Closing Q&A

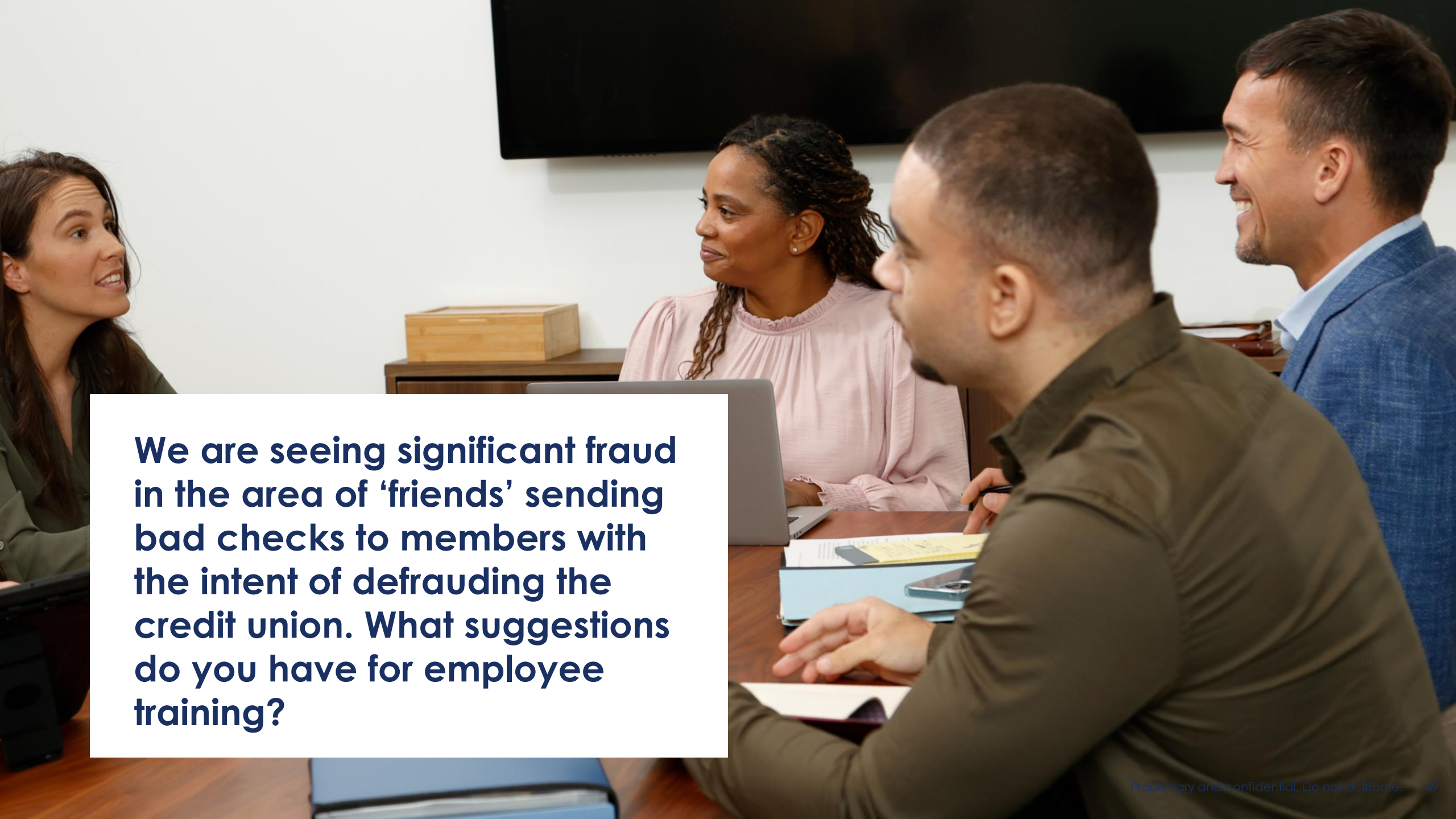
→ Use the online Q&A functionality to submit questions for any of the presenters on today's Risk Forum

→ You can also reach out to our TruStage™ Risk Consultants at **800.637.2676** or by email at **riskconsultant@trustage.com**






When members are victims of scams, is there an obligation to reimburse or assist them in recovery?

A photograph of four people (three men and one woman) sitting around a wooden table in a meeting. They are all looking towards the left side of the frame. The woman on the far left is speaking. The man next to her is listening. The man in the foreground is looking down at a laptop. The man on the far right is smiling. There is a white text box overlaid on the left side of the image.


We are seeing significant fraud in the area of ‘friends’ sending bad checks to members with the intent of defrauding the credit union. What suggestions do you have for employee training?

What best practices can you share to educate members regarding scams and fraud?





What measures can we take to better protect our elderly members from fraud – especially when we know they are being scammed?

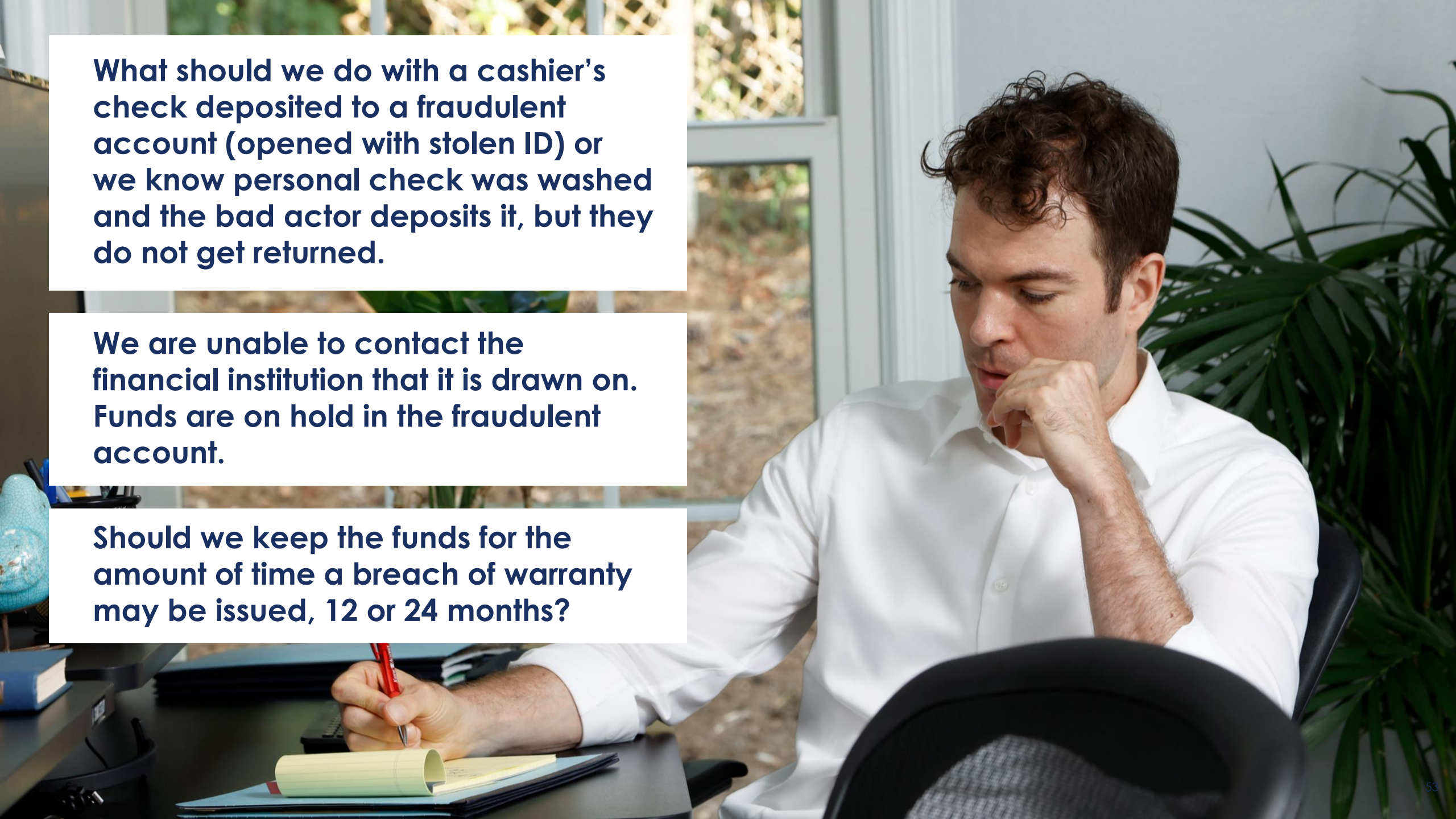
A woman with blonde hair is seen from the side, facing a male teller. The teller is wearing a dark suit, a white shirt, and a red patterned tie. He is standing behind a counter and looking at the woman. The background shows a typical bank interior with shelves and a pen holder.


We are hearing more about in-person impersonations with fraudsters performing transactions at the teller line. Do you have any signs that we should be on the lookout for?

What should we do with a cashier's check deposited to a fraudulent account (opened with stolen ID) or we know personal check was washed and the bad actor deposits it, but they do not get returned.

We are unable to contact the financial institution that it is drawn on. Funds are on hold in the fraudulent account.

Should we keep the funds for the amount of time a breach of warranty may be issued, 12 or 24 months?





**What trends or risks should we
be on the lookout for related to
online account fraud?**

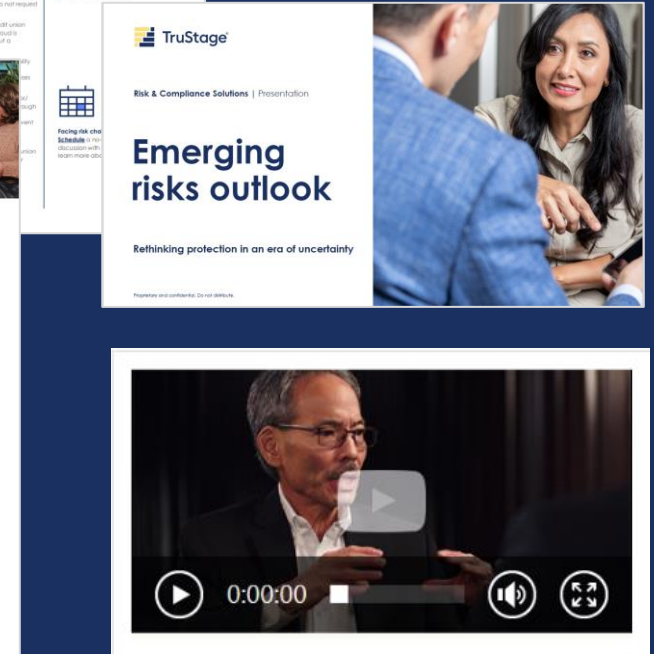
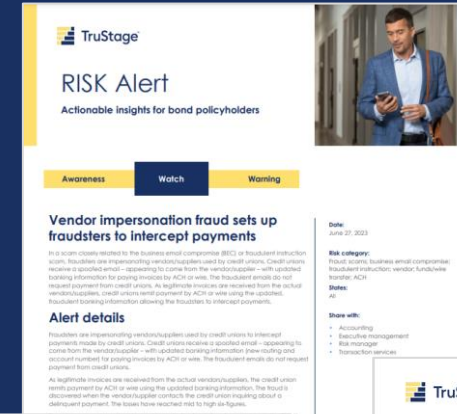
Risk resources

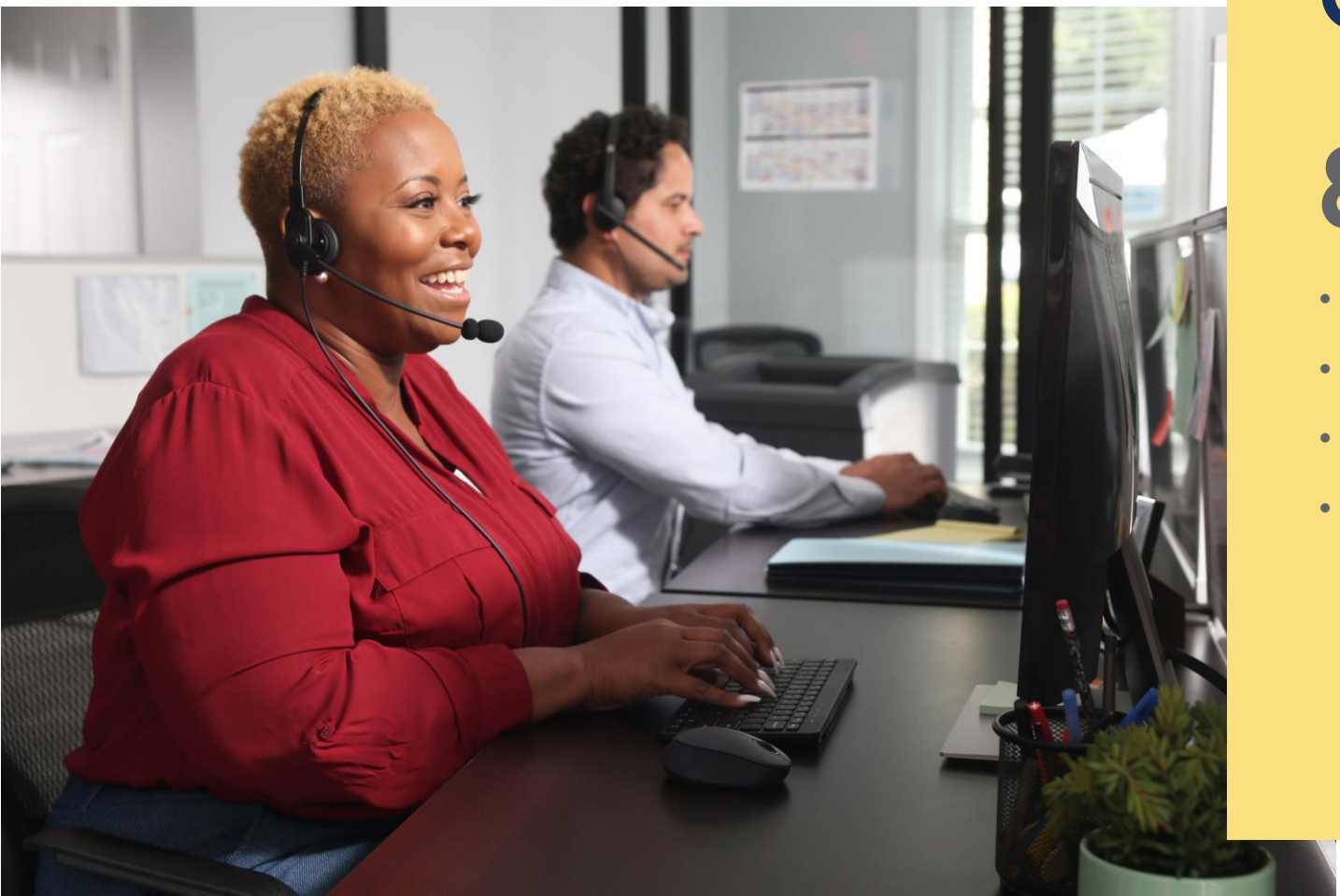
Business Protection Resource Center www.trustage.com/bprc

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

“Great webinars - serious, important information delivered in a relaxed, ‘we’re among friends’ way.”

\$9B 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](#)

Business Protection Solutions Claims

Online:

<https://www.trustage.com/login/my-services>

Claims Response Line:

844.377.5828

Monday-Friday 7:00 am – 5:00 pm CST

Emergency claims can still be reported
outside of normal business hours.





Thank you.

Contact

Risk & Protection Solutions

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.