TruStage®

Risk & Compliance Solutions | WI CU Connect

Emerging Risks

Rise above your risks

Risks are evolving

Careful risk identification, effective risk management and the need for strategy is even more critical

- Exploding diversity of risk combines with an increasingly volatile environment
- More places for risk indicators to hide
- Constrained risk management resources

Top-of-mind emerging risks

While each credit union has its own unique footprint; these emerging risk trends should be on your radar:

- ITM fraud
- Treasury check fraud
- Money mule accounts & account-to-account transfers
- ATM Jackpotting

Interactive teller machine (ITMs) targeted by fraudsters

- ITM fraud exploded in 2023
- Mid six-figure losses are common – with a few seven-figure losses
- Fraudsters targeting the self-serve feature at outside ITMs during non-business hours to withdraw funds from member accounts
- Counterfeit debit cards used to authenticate members OR account number plus SSN or DOB
- Fraudsters hit their pot of gold when the member has a HELOC – more money to steal

ITM risks

Some losses exceeding $500,000

Traditional ATM

- Use of counterfeit debit card
- Skimming/shimming risk

Video assistance teller

- Very little risk
- Be aware of deepfakes and use proper forms of identification that can be scanned into the ITM

Self-service option

- Most risky
- Available 24/7
- Using easily identifiable information that can be compromised
- Using debit card to authenticate member-counterfeit cards easily used and created by skimmers or shimmers

ITM fraud mitigation tips

In general

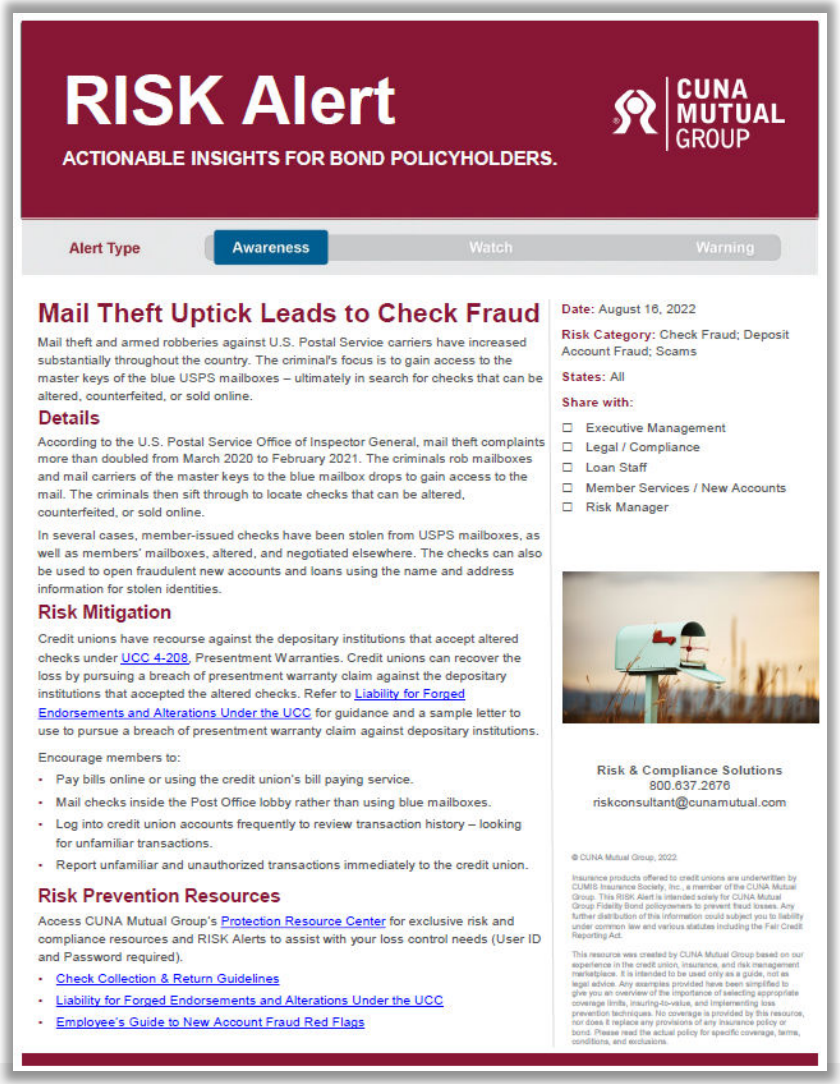
- Block all fallback transactions at ITMs and ATMs
- Set low daily dollar limits
- Use skimming/shimming detection technology
- Conduct daily inspections of all ITMs/ATMs – including opening to inspect for deep shimmers
  - If foreign device or tampering is detected- machine should automatically shut down
- Require additional forms of ID to be scanned
- Do not allow access to line of credit accounts (i.e. HELOC)
- Ensure all ITMs and ATMs are EMV enabled
- Educate members of risk at ITM/ATMs-report any signs of tampering

For self-service options

- Do not use easily compromised identification to access accounts (i.e.: SSN, DOB, Account number)
- If debit card is used to authenticate; ensure ITM reads the EMV/chip card, if it is not detected decline transaction
  - Do not allow fallback transactions
- Set low daily dollar limits for withdrawals
  - One transaction per day
- Implement one-time passcodes sent to their device before proceeding with transaction access
- Limiting hours of operations for self-service option and require member to use video teller if available
- Review reports daily-velocity of transactions – is this normal activity? Should be done in the morning

Mail theft fuels check fraud

- Thieves have been stealing mail out of blue drop boxes
- Steal members' issued checks
  - ✓ Alters the payee and dollar amount on the original items and negotiates them elsewhere
  - ✓ Manufacture fraudulent checks using information from member's legitimate check
- 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 depositary institutions
- Credit unions take the loss from fraudulent checks created using information from members' legitimate checks
  - ✓ Checks must be returned by the credit union's midnight deadline



RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

Alert Type: Awareness | Watch | Warning

Mail Theft Uptick Leads to Check Fraud

Mail theft and armed robberies against U.S. Postal Service carriers have increased substantially throughout the country. The criminal's focus is to gain access to the master keys of the blue USPS mailboxes – ultimately in search for checks that can be altered, counterfeited, or sold online.

Details

According to the U.S. Postal Service Office of Inspector General, mail theft complaints more than doubled from March 2020 to February 2021. The criminals rob mailboxes and mail carriers of the master keys to the blue mailbox drops to gain access to the mail. The criminals then sift through to locate checks that can be altered, counterfeited, or sold online.

In several cases, member-issued checks have been stolen from USPS mailboxes, as well as members' mailboxes, altered, and negotiated elsewhere. The checks can also be used to open fraudulent new accounts and loans using the name and address information for stolen identities.

Risk Mitigation

Credit unions have recourse against the depositary institutions that accept altered checks under UCC 4-208, Presentment Warranties. Credit unions can recover the loss by pursuing a breach of presentment warranty claim against the depositary institutions that accepted the altered checks. Refer to Liability for Forged Endorsements and Alterations Under the UCC for guidance and a sample letter to use to pursue a breach of presentment warranty claim against depositary institutions.

Encourage members to:

- Pay bills online or using the credit union's bill paying service.
- Mail checks inside the Post Office lobby rather than using blue mailboxes.
- Log into credit union accounts frequently to review transaction history – looking for unfamiliar transactions.
- Report unfamiliar and unauthorized transactions immediately to the credit union.

Risk Prevention Resources

Access CUNA Mutual Group's Protection Resource Center for exclusive risk and compliance resources and RISK Alerts to assist with your loss control needs (User ID and Password required).

- Check Collection & Return Guidelines
- Liability for Forged Endorsements and Alterations Under the UCC
- Employee's Guide to New Account Fraud Red Flags

Date: August 16, 2022

Risk Category: Check Fraud; Deposit Account Fraud; Scams

States: All

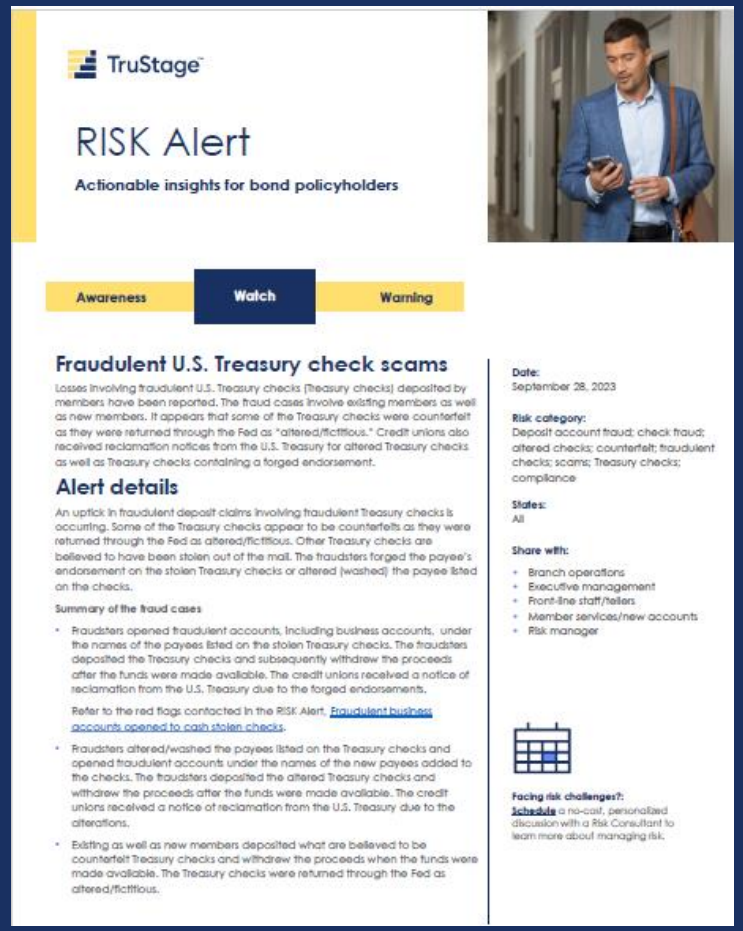
Share with:

- ☐ Executive Management
- ☐ Legal / Compliance
- ☐ Loan Staff
- ☐ Member Services / New Accounts
- ☐ Risk Manager

Risk & Compliance Solutions
800.637.2676
riskconsultant@cunamutual.com

Fraudulent U.S. Treasury checks

- Significant increase in losses - many in the six-figure range
- Counterfeit, forged (endorsement), and altered Treasury checks
- Primarily involves new account fraud
  - Fraudsters open accounts in the name of the payees, including businesses or
  - Alter/wash payee – replaced with fraudster's name
- Altered Treasury checks as well as Treasury checks with forged endorsements are generally subject to reclamation
- Treasury has one year to pursue a check reclamation for a breach of presentment guarantee by credit union
- Can be extended by an additional 6 months (18 months total) if the payee provides notice of the forged endorsement within one year of issuance



TruStage

RISK Alert

Actionable insights for bond policyholders

Awareness | Watch | Warning

Fraudulent U.S. Treasury check scams

Losses involving fraudulent U.S. Treasury checks (Treasury checks) deposited by members have been reported. The fraud cases involve existing members as well as new members. It appears that some of the Treasury checks were counterfeit as they were returned through the Fed as "altered/fictitious." Credit unions also received reclamation notices from the U.S. Treasury for altered Treasury checks as well as Treasury checks containing a forged endorsement.

Alert details

An uptick in fraudulent deposit claims involving fraudulent Treasury checks is occurring. Some of the Treasury checks appear to be counterfeits as they were returned through the Fed as altered/fictitious. Other Treasury checks are believed to have been stolen out of the mail. The fraudsters forged the payee's endorsement on the stolen Treasury checks or altered (washed) the payee listed on the checks.

Summary of the fraud cases

- Fraudsters opened fraudulent accounts, including business accounts, under the names of the payees listed on the stolen Treasury checks. The fraudsters deposited the Treasury checks and subsequently withdrew the proceeds after the funds were made available. The credit unions received a notice of reclamation from the U.S. Treasury due to the forged endorsements.

  Refer to the red flags contacted in the RISK Alert, Fraudulent business accounts opened to cash stolen checks.

- Fraudsters altered/washed the payees listed on the Treasury checks and opened fraudulent accounts under the names of the new payees added to the checks. The fraudsters deposited the altered Treasury checks and withdrew the proceeds after the funds were made available. The credit unions received a notice of reclamation from the U.S. Treasury due to the alterations.

- Existing as well as new members deposited what are believed to be counterfeit Treasury checks and withdrew the proceeds when the funds were made available. The Treasury checks were returned through the Fed as altered/fictitious.

Date:
September 28, 2023

Risk category:
Deposit account fraud; check fraud; altered checks; counterfeit; fraudulent checks; scams; Treasury checks; compliance

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 to learn more about managing risk.

U.S. Treasury check verification

- Use the Treasury Check Verification System (TCVS) - https://tcvs.fiscal.treasury.gov/
  - Will verify whether Treasury check was issued
  - Does not verify payee
- Verify by email
- U.S. Treasury Inspector General for Tax Administration: checkintegrity@tigta.treas.gov
- U.S. Treasury's Bureau of Fiscal Service: payments@fiscal.treasury.gov
- Include the following:
  - Date of check
  - Serial number
  - Amount
  - Payee
  - Routing number
  - Paste image of Treasury check into body of email
- Response will indicate whether payee has been altered

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

The Trend

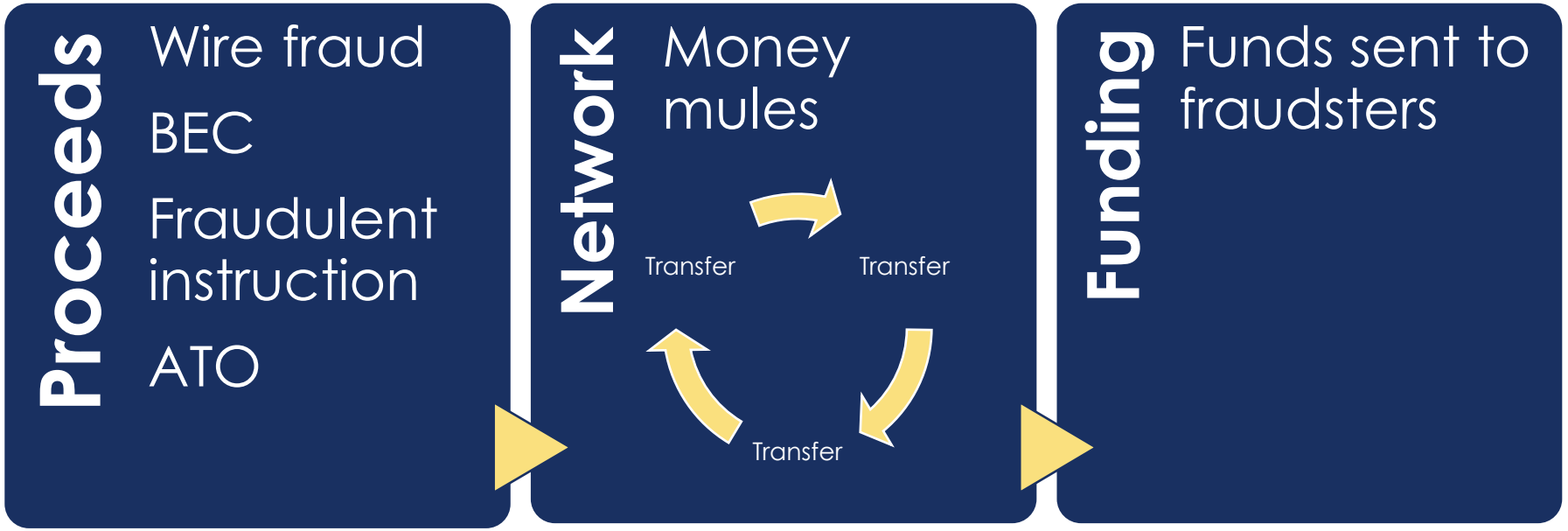
Account takeovers/money mules

- Account takeovers and transfers to money mule accounts occur at the same credit union
- Fraudsters recruit money mules to open fraudulent accounts at target credit union
- Members scammed into providing their login credentials to fraudsters
- Fraudsters use member-to-member transfer feature to transfer funds to money mule accounts
- Money mules withdraw funds through various means

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)

Money mules' role in laundering stolen funds

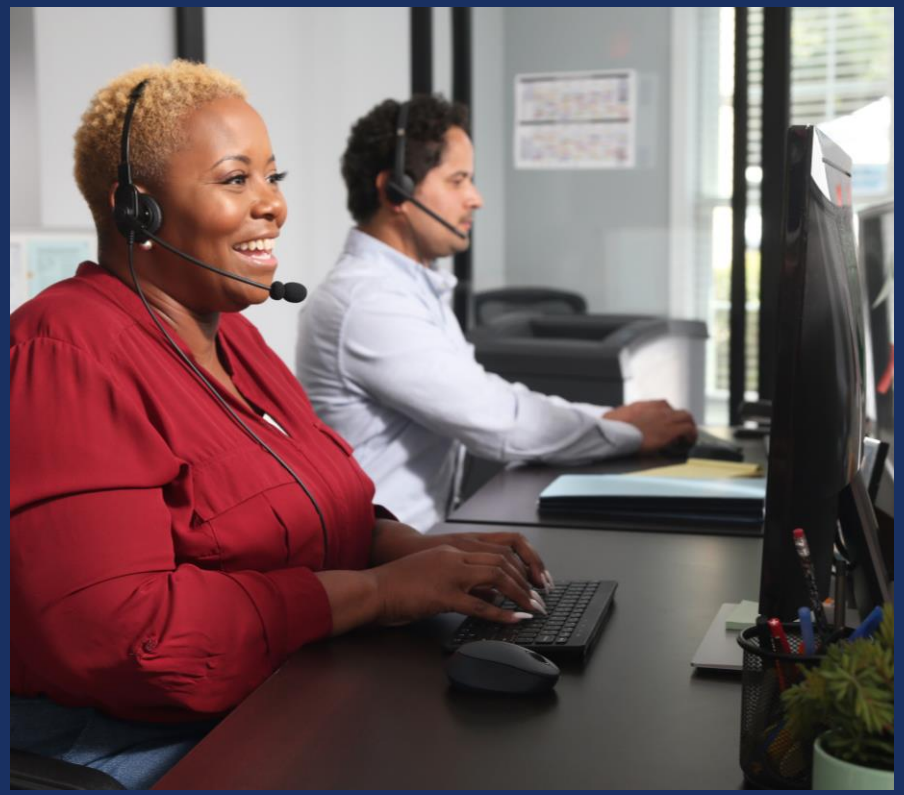


- Fraudsters recruit money mules to help launder proceeds derived from criminal activities
- May open fraudulent accounts using synthetic identities
- Adds layers of recipients to the money trail
- Complicates law enforcement's ability to trace money from a victim to criminal actor

Account takeover: Money mules

$1M loss impact

- Fraudsters recruited money mules to open fraudulent accounts at the credit union
- Members were victimized in a P2P/Zelle-like scam allowing fraudsters to re-set their passwords and login to their accounts
- Fraudsters used member-to-member transfer feature to make large dollar transfers from compromised accounts to money mule accounts
- Money mules withdrew proceeds through various means – in-person withdrawals, ATM, POS gift card purchases, P2P, etc.



Risk mitigation

- Warn members of scams to obtain login credentials and debit card details – consider a special mailer
- Deploy an identity verification solution capable of detecting synthetic identities
- Don’t allow members to use the “forgot password” feature using unregistered devices
- Require signed authorizations before allowing member-to-member transfers
- Implement reasonable monetary limits for member-to-member transfers – single transaction limit, daily limit and weekly limit

ATM jackpotting

ATM jackpotting methods (requires physical access to the ATM)

Malware

Fraudsters typically insert a flash drive containing malware into the ATM's internal USB port. The malware then issues dispense commands to the ATM causing the machine to dispense cash.

Black box/Laptop

Fraudsters connect a black box (laptop) directly to the ATM dispenser. The fraudster uses the black box to send dispense commands to the ATM dispenser.

Man-in-the-middle (MiTM)

Fraudsters install a device between the ATM's computer and the network cable connection to the acquirer's host system. Messages from the acquirer's host system are intercepted and modified specific to the card being used by the fraudster.

Physical access to ATMs

- Fraudsters may dress as an ATM technician and physically access the ATM
- Opens top hat with a generic key purchased online OR drills hole (about the size of a golf ball) near the PIN pad to gain access (covers the hole with decal)
- Inserts flash drive containing malware to the ATM's USB port OR connects black box to the ATM's dispenser
- Fraudster issues command to ATM to dispense cash
- Money mules are used to collect the cash

ATM jackpotting: Risk mitigation

- Work with ATM vendor
- Replace locks on ATM top hats
- Equip top hat with alarm
- Encrypt ATM hard drivers
- Encrypt communication between the ATM and the acquirer's host system
  - ✓ If a router is used, the communications link between the ATM and the router must be protected
- Install security patches when made available
- Send a technician to any ATM that has been offline for at least 5 minutes
- Frequent inspections

Emerging risk outlook

Loss & litigation trends

- Recessionary trends (fraud; dishonesty; employment matters; delinquencies)
- ATM smash 'n grab
- Slips, trips & falls
- Defective repossession notices
- Overdraft/NSF fees
- Member discrimination

Fraud & scams

- Check fraud/mail theft
- Ransomware; BEC; fraudulent instruction
- P2P/Zelle fraud
- New account/ account takeover fraud
- Loan fraud
- Member scams / Elder exploitation

Cyber oversight

- Cyber & the c-suite
- Authentication
- Ransomware & scams
- Phishing, smishing & ChatGPT
- Vendor oversight
- Cyberthreat technology
- Staff training

Reg & compliance

- Constant change
- Consumer protection (Overdraft/NSF fees; Junk fees; Reg E; UDAAP; fair lending; ADA & website accessibility; wiretap)
- FCRA
- Marijuana banking
- Data privacy

Workplace safety

- Active assailant incidents
- Workplace violence – employee or member
- Encampment/ vagrancy
- Office opening & closing
- Policies & procedures
- Employee training

Human capital

- Flexible work arrangements
- Diversity, equity & inclusion
- Talent & skills – cyber; strategic thinking; gaps & shortages
- Succession planning
- Recruiting/retention

Branch of the future

- Open branches/micro-branches
- Member engagement
- Virtual banking; live chat agents
- Metaverse
- Remote work arrangements
- Universal banker employees

Business operations

- Weather events
- Business continuity planning
- Climate change - impact on financial, members & loan collateral
- Corporate & social responsibility
- Internal controls

Disruptive technology

- Artificial intelligence
- Video banking (ITMs)
- ATMs with advanced transaction capabilities
- Cryptocurrency
- Fintech relationships (losing relevance)
- Non-traditional financial institutions

Risk governance

- Integrating risk decisioning with strategy
- Acceleration of digital technology integration
- Third-party and fourth-party vendor oversight
- Geopolitical influence
- Volatile environment
- Resource constraints

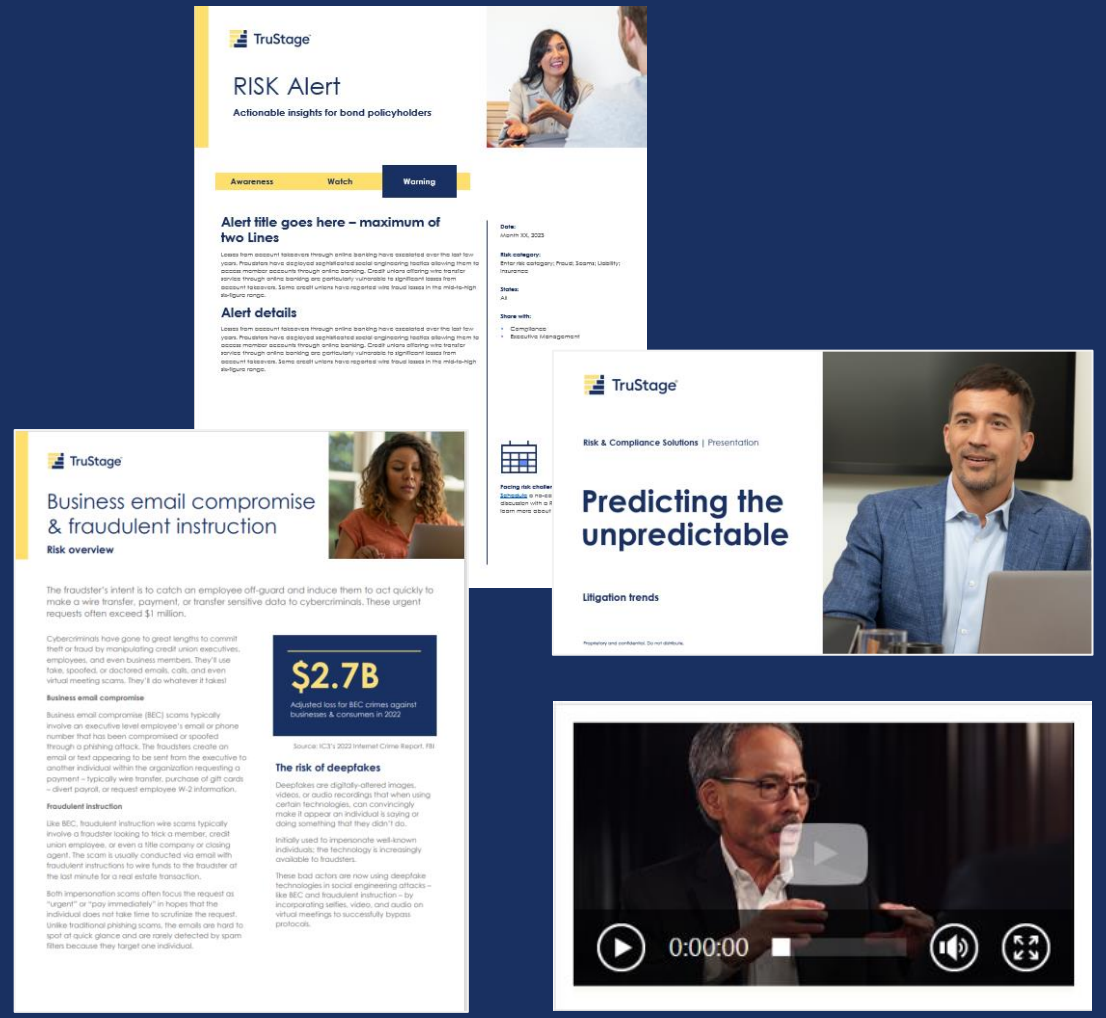
Risk resources

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



1:1 risk consultations

Helping you make confident decisions by sharing loss control guidance, relevant peer insights, and proven practices.

800.637.2676

riskconsultant@trustage.com

TruStage®

Thank you.

Contact information
Kenneth.otsuka@trustage.com
Office: 608.665.5168
Mobile: 847.612.9653