



Risk & Compliance Solutions | Webinar

---

# TOP

emerging risks in 2025

---

**The unpredictability of the future**

Proprietary and confidential. Do not distribute.



# TruStage™ Risk Management panelists



**Jim Bullard**  
Senior Risk Consultant  
Georgia



**Chris R. Gill**  
Senior Manager  
Maryland



**Brad Neumann**  
Senior Risk Consultant  
Wisconsin



**Ken Otsuka**  
Senior Risk Consultant  
Illinois

Don't let not knowing which emerging risks  
are around the corner take the blame.

# Risks are evolving

- Exploding diversity of risk combines with an increasingly volatile environment
- Vague, chaotic and constantly changing
- More complex – impacting many factors or processes simultaneously
- More places for risk indicators to hide

**Emerging risks**

**New** - recently introduced or unforeseen

**Evolving** - becoming more impactful in frequency or severity

**Well-known** – familiar or obvious risk/loss

**Objectives**  
Where are we going?



**Risks**  
What could go right / wrong?

**Initiatives**  
How do we get there?

# Concerning credit union loss patterns



Unfortunately, six- and seven-figure losses are impacting credit unions across the country

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

→ Many of these large losses are occurring within well-known risk areas and their frequency & severity can be significantly minimized with proper loss controls.





# On the radar



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

- Account takeovers
- Consumer protection
- Data privacy & protection
- Fraudulent checks/deposits
- Human error/social engineering
- Incident planning
- ITMs & ATMs
- Loan fraud
- Vendor incidents
- Workplace safety



Tier 1 risk with significant loss potential

# Account takeovers

- **Probability:** Frequent
- **Severity:** Critical
- **Primary control:** Secure form of 2-factor authentication / Fraud monitoring

# Account takeovers



- Members scammed out of their login credentials in SMiShing and Vishing campaigns
- Fraudsters typically target the "forgot password" feature – triggers a 2FA passcode to member who provides it to the fraudster
- In some cases, the fraudulent text messages contain a link to a spoofed site made to appear as the online banking login page – members enter login credentials plus 2FA passcodes
- Recent trend has the account takeovers and money mule accounts at the same credit union



- Don't allow members to use the "forgot password" feature with an unregistered device
- Deploy a more secure form of 2-factor authentication, such as a token or push notifications
- Ensure transaction limits, including member-to-member transfers, are reasonable
- Temporarily disable payment type targeted by fraudsters
- Deploy a real-time fraud monitoring solution that leverages AI and machine learning
- Retain vendor to take down spoofed websites
- Member education





Tier 3 risk with losses anticipated

# Consumer protection

- **Probability:** Occasional
- **Severity:** Critical
- **Primary control:** Compliant processes



# Consumer protection



## Reg E

- Some credit unions may not be willing to re-credit members in account takeover cases
- Proposed amendments to the EFTA (Protecting Consumers from Payment Scam Act)

## Fair Lending

- The focus on Fair lending compliance has increased in recent years - as evidenced by CFPB and NCUA guidance.
- Regulatory agencies consider that;  
Discretion = Risk



- Ensure appropriate staff receive training on Reg E
- Includes all aspects of lending including: marketing, pricing, underwriting, and loan servicing
- Governing regulations:
  - ECOA
  - FHA
  - HMDA
  - FCRA





Tier 3 risk with losses anticipated

# Data privacy & protection

- **Probability:** Occasional
- **Severity:** Critical
- **Primary control:** Compliance program

# Data privacy & protection



With the increased focus on consumer data rights, more litigation is quickly becoming a significant risk to credit unions resulting from consumers who claim they have suffered damage as a result of a cybersecurity attack

- Ransomware
- Business email compromise/ fraudulent instructions
- Scams against members



- Ensure that established governance policy and objectives are compatible with the strategic direction
- Confirm governance policies and objectives are communicated to all relevant parties
- Practice good security hygiene
- Take proactive measures to protect data
- Foster a culture of responsibility and security across the organizations





Tier 1 risk with significant loss potential

# Fraudulent checks/deposits

- **Probability:** Frequent
- **Severity:** Critical
- **Primary control:** Employee training

# Fraudulent checks/deposits



## Fraudulent checks clearing member accounts

- Stolen mail problem fueled the increase in check fraud
- Fraudsters steal members' issued checks
- Fraudsters alter the checks (payee) or manufacture fraudulent checks using information from members' stolen checks

## Fraudulent deposits

- Also fueled by stolen mail problem
- Fraudulent U.S. Treasury checks are a huge problem



- Pursue breach of presentment warranty claims against FIs that accept members' altered checks
- Ensure members report unauthorized checks within the specified time frame in account agreement
- Review large dollar checks presented for payment
- Be wary of large dollar Treasury checks presented by new members
- Place holds in accordance with Reg CC or deposit to savings account for a longer hold
- Verify security features; TCVS and verify payee







Tier 1 risk with significant loss potential

# Human error/social engineering

- **Probability:** Frequent
- **Severity:** Marginal
- **Primary control:** Employee training

# Human error/social engineering



## Types of social engineering

- Phishing
- Vishing
- SMiShing
- Impersonation fraud



- Require redundancies
- Anti-virus/Anti-malware software
- Multi-factor authentication
- Limit public information
- Safe-guarding tools
- Penetration and social engineering tests
- Employee and member education





Tier 2 risk with significant loss potential

# ITMs & ATMs

- **Probability:** Probable
- **Severity:** Critical
- **Primary control:** Physical security/Prohibit fallback transactions

An **EXAMPLE**

# The evolution of ATM risk...



# ITMs & ATMs



## ITM fraud

Fraudsters are using the self-service feature to withdraw funds from member accounts – primarily using counterfeit debit cards. In some cases, deep insert skimmers were found on ITMs.

## ATM jackpotting

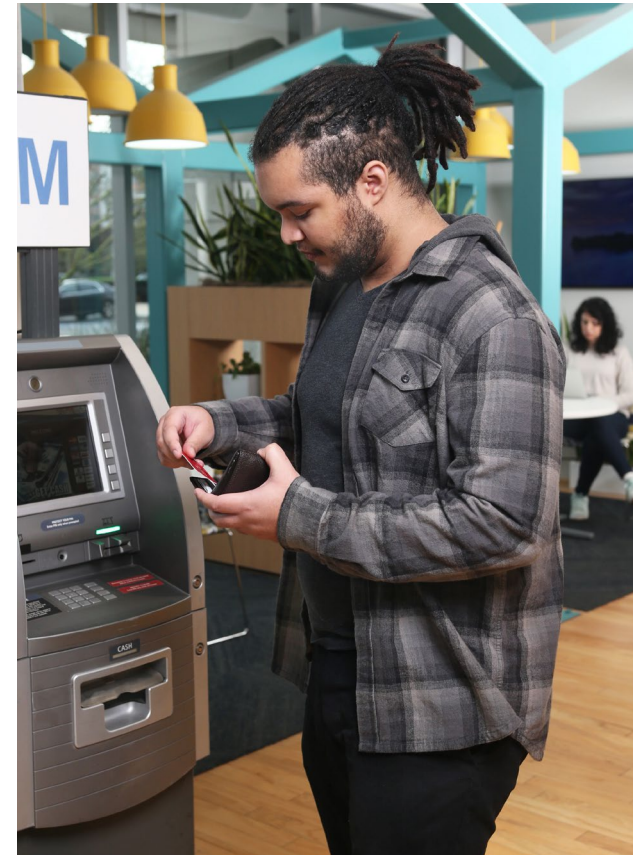
Fraudsters infect ATMs with malware causing the machines to dispense currency

## ATM smash 'n grabs

A resurgence in ATM burglaries where criminals use a blow torch or other forced entry to open the ATM's money chest or steal it altogether.



- Don't allow fallback transactions
- Don't allow access to line-of-credit loans using the ITM's self-service feature
- Reduce the currency stored in the machines
- Replace lock on ATM top hat and install alarm on top hat
- Install GPS trackers
- Install a security gate around machine
- Alarm with door, heat, seismic, audible alarm and strobe light
- Daily inspections and Increase camera coverage







Tier 2 risk with anticipating loss

# Loan fraud

- **Probability:** Likely
- **Severity:** Marginal
- **Primary control:** Employee training

# Loan fraud



## Loan application fraud

- Identity Theft
- Synthetic ID Fraud
- Employment verification
- Loan Stacking

## Collateral fraud

- Vehicle title fraud
- Solar lending



- Fraud detection service
- Verify the match of name, address, phone, SSN, tax ID, and date of birth against public/private databases
- Use out of wallet questions - KBA
- Out-of-band phone verification
- Geolocation/triangulation
- Vehicle title verification service
- Vendor due diligence





Tier 1 risk with significant loss potential

# Third-party vendors

- **Probability:** Occasional
- **Severity:** Critical
- **Primary control:** Continuous vendor oversight

# Third- and N<sup>th</sup>-party vendors



- Governing third-parties in the data supply chain is critical
- Supply chain attacks make it easier for bad actors to circumvent security controls
- A single compromise could impact hundreds of companies and customers
- **73% of total reported incidents** since September 1, 2023 involved compromises with a third-party service provider (NCUA)



- Identify your vendors and their vendor/partners and be aware of what type of access they have to credit union and member data
- Understand their data security standard, practices, and controls
- Establish expectations and obligations within a written contract
- Know the vendors' policies on reporting data breaches and suspected incidents
- Ask them critical questions



# Questions for critical vendors



- Who is responsible for cybersecurity within the vendor organization?
  - Does the vendor outsource any IT or IT security functions to third-party service providers? If so, who, what do they do, and what type of access do they have?
  - Have you identified any other third parties who have access to your network or data? How do you oversee their security initiatives?
  - How does the vendor plan and train for a cybersecurity incident?
  - How does the vendor continuously assess and remediate cyber vulnerabilities?
  - What processes does the third party have in place to prevent the exfiltration of sensitive data?
- Does the third party have data recovery capability?
  - Specifically, how does the third party protect customer information?
  - What types of physical protection are in place to prevent unauthorized access to data or infrastructure assets?
  - Does the third-party vendor have a disaster recovery plan that includes a cyber incident response plan?
  - Has the third party experienced a significant cyber incident or been named in a related lawsuit?
  - Describe the process to communicate security incidents affecting our organization's data.



Tier 3 risk with growing concern

# Workplace safety

- **Probability:** Remote
- **Severity:** Negligible
- **Primary control:** Safety plan; employee training



# Workplace & employee safety



- Abusive members
- Active assailant incidents
- Common office risks
  - Slip, trip & falls
  - Lifting/handling
  - Ergonomics
- Disaster response
- Remote work environment
- Robbery



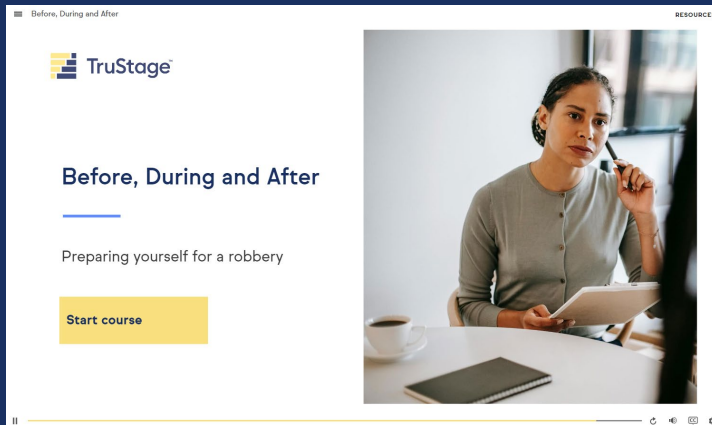
- Prioritizing violence prevention efforts is not only the right thing to do; it is also required under Section 5(a) (1) the General Duty Clause of the OSHA Act of 1970
- A work environment free from recognized hazards that are causing or are likely to cause death or serious physical harm
- Develop & maintain written safety program
- Employee safety orientation & ongoing workplace prep training
- Prevention through self-inspection – everyone is a risk manager



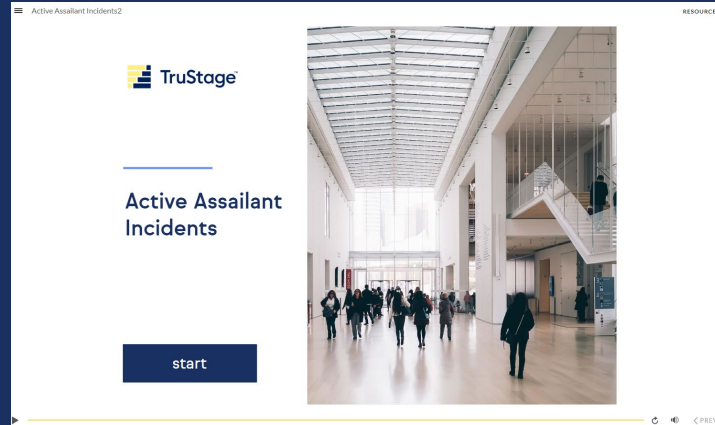
Proactively address your safety culture so your employees have the right safety mindset

# Employees: your first line of defense

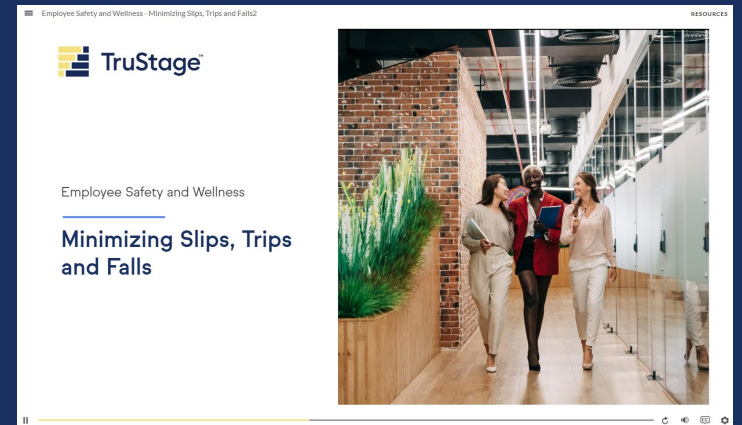
## Interactive training modules



[www.trustage.com/robbery-prep](http://www.trustage.com/robbery-prep)



[www.trustage.com/active-shooter](http://www.trustage.com/active-shooter)



[www.trustage.com/employee-safety](http://www.trustage.com/employee-safety)

[www.trustage.com/risk-training](http://www.trustage.com/risk-training)

No-cost • No User ID/Password • 20-30-minute learnings • Test your knowledge • Completion certificates



Tier 2 risk with growing loss concern

# Incident planning

- **Probability:** Occasional
- **Severity:** Marginal
- **Primary control:** Plan testing & preparedness

# Incident planning



Assess the performance of your business resilience programs

Take steps to ensure that the structure and strategies are in place to anticipate and respond to the next event, no matter what it may be.

Emphasize speed and flexibility, so you are able to quickly adapt to rapid change



- Prioritize critical disrupters to core functions– like the potential convergence of events
- Ensure current service levels can be maintained and determine maximum allowable downtimes
- Testing your plan can be a sure-fire way to find the gaps in your business resiliency plan prior to an interruption
- Include multiple level of employees



# Tabletop/scenario testing tips

1. Review supporting documents needed to test your incident plan
2. Identify your exercise planning team – facilitator; participant; observer; and evaluator
3. Gain agreement regarding exercise concept (scope, type, mission, exercise priorities), exercise objectives, core capabilities, and timeline
4. Hold an initial planning meeting. Determine if you'll organize as a single group or use a multi-table format organized by functional area
5. Coordinate logistics and select the scenario
6. Ensure all exercise elements are ready and Be sure to resolve any open planning issues
7. Make documents available for each participant
8. Conduct the exercise
9. Ensure the discussion is focused on the objectives and issues within the time allotted

The end goal is to produce an after-action report with recommendations for improving preparedness capabilities with timelines for implementation and assigned responsible parties.



**TruStage**

## Business resilience

### Planning guide & checklist

Business challenges have provided organizations an opportunity to reclaim and reinvigorate business resilience planning. While there is no one correct way to perform resilience planning; it is important to continuously improve the plan by incorporating lessons learned.

Credit union leaders need to assess the performance of their business resilience programs and take steps to ensure that the structure and strategies are in place to anticipate and respond to the next event, no matter what it may be.

**Plans must emphasize speed and flexibility, so you are able to quickly adapt to rapid change.**

It is also essential that leadership and employees are given fact-based information and tested alternatives to enable real-time decision making. This integrated, comprehensive approach will help build long-term operational resilience and prepare the credit union organization for any future disruption.

Clearly, there is a lot at risk without business resilience planning. It is critical to give everyone a reason to get involved and play their part in business resilience. It is to your advantage to adopt a long-term view of business operations and investments.

#### Critical building steps

Establish a core vision that is tailored to your credit union's specific business objectives, priorities, existing future state business models. Recognize and understand the vulnerabilities and potential business impact.

Focus must go beyond vision and theory; you need application. Operational resilience can be strengthened by identifying the potential events that could affect your business, grading risks according to the impact, and then implementing a strategy to mitigate and manage risks.

Finally, your employees are crucial to the resilience of the credit union. Providing people with the tools and skills required to adapt to change will contribute to improved resilience.

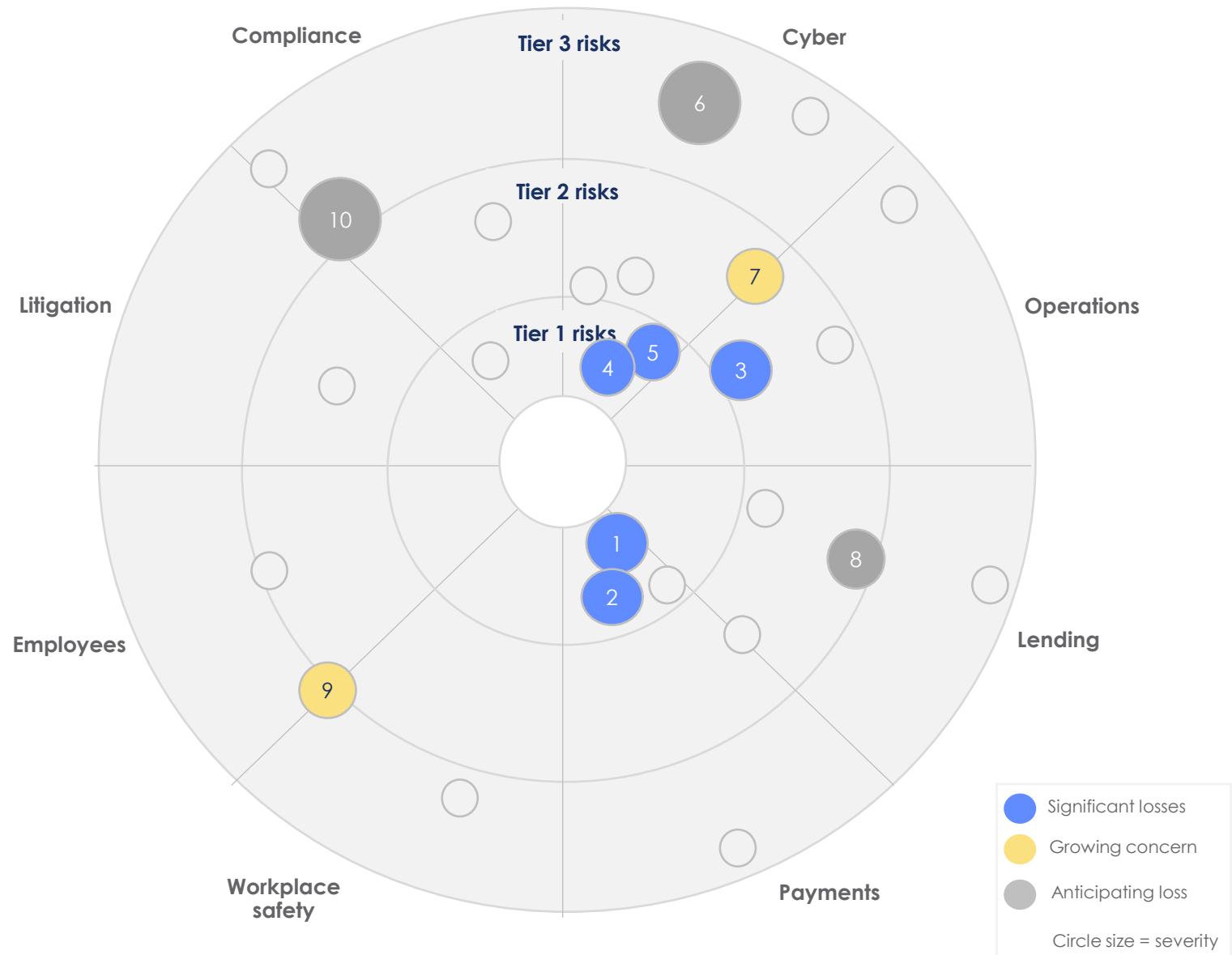
- Foster a resilient culture
- Develop resilient team members
- Revisit strategic objectives and business model
- Assess risk and identify potential disruptors
- Measure effectiveness through testing



# Plotting emerging risks

1. Account takeovers
2. Fraudulent checks/deposits
3. ITMs/ATMs
4. Human error/social engineering
5. Vendor incidents
6. Data privacy & protection
7. Incident planning
8. Loan fraud
9. Workplace safety
10. Consumer protection

\*Numbers indicate risk not rank





# Other emerging risks on the radar

- New account fraud
  - Wire fraud
  - Member scams
  - Fraudulent instruction; Business email compromise; vendor impersonation
  - Ransomware
  - Artificial intelligence & deepfakes
  - Internal controls & employee fraud
- Climate change-related risks
  - Solar lending
  - Collections & defective repossession notices
  - Overdraft/NSF fees litigation
  - Employee retaliation; discrimination
  - Employee recruiting & retention
  - Real-time payments
  - Social engineering & phishing

When risk management is effective, typically nothing bad happens. And, it is difficult to show the value of nothing. But if you're blindsided by a problem, your bottom-line and reputation usually takes the hit. Don't let not knowing which emerging risks are around the corner take the blame.



# Contact us

## 800.637.2676

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

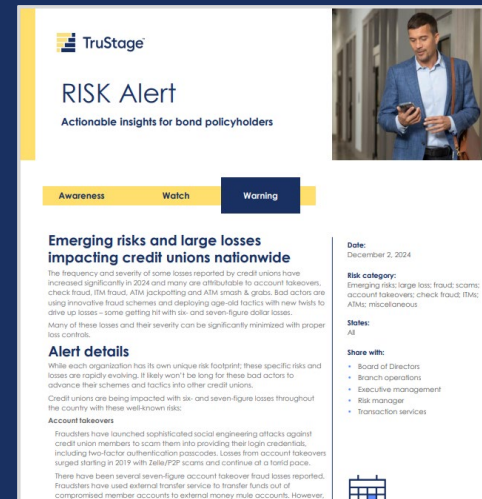
# Risk resources

**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**

**Emerging risks and large losses impacting credit unions nationwide**

The frequency and severity of some losses reported by credit unions have increased significantly in 2024 and many are attributable to account takeover, check fraud, ATM fraud, ATM jacking/popping and ATM smash & grabs. Bad actors are using innovative fraud schemes and deploying age-old tactics with new twists to drive up losses – some getting hit with six- and seven-figure dollar losses. Many of these losses and their severity can be significantly minimized with proper loss controls.

**Alert details**

While each organization has its own unique risk footprint, these specific risks and losses are rapidly evolving. It likely won't be long for these bad actors to advance their schemes and tactics into other credit unions. Credit unions are being impacted with six- and seven-figure losses throughout the country with these well-known risks:

**Account takeovers**

Fraudsters have launched sophisticated social engineering attacks against credit union members to scam them into providing their login credentials, including two-factor authentication passcodes. Losses from account takeovers surged starting in 2019 with Zelle/P2P scams and continue of a rapid pace. There have been several seven-figure account takeover fraud losses reported. Fraudsters have used external transfer services to transfer funds out of compromised member accounts to external money mule accounts. However,

**Date:** December 2, 2024

**Risk category:** Emerging risks, large loss fraud, scams, account takeovers, check fraud, ATM, ATM; miscellaneous

**States:** All

**Share with:**

- Board of Directors
- Branch operations
- Executive management
- Risk manager
- Transaction services



**TruStage**  
**TOP**  
 emerging risks in 2025

While each organization has its own unique risk footprint, risks are rapidly evolving and so must the strategic conversation with risk and compliance in mind. Unfortunately, risks and losses fluctuate at the same time bad actors produce new innovative tactics deploying age-old schemes – quite often with new twists.

Emerging risks can typically be categorized as – new, evolving, and well-known – however, no matter the placement they can impact your financial stability, disrupt business strategy, and damage your reputation.

**New risks** are recently introduced or unforeseen altogether. Think of risks related to the autonomous vehicles, climate risk, and even active assailant incidents – these threats provide little certainty and may be difficult to understand their significance.

**Evolving risks** are not always new but appear to be impacting more organizations as time goes on. Risks related to business email compromise, overdraft/NSF fee litigation, and remote work arrangements are examples.

**Well-known risks** are typically those that are repeat offenders – areas where loss frequency and severity are consistent. These risks have usually been around for some time.

Unfortunately, six- and seven-figure losses from relatively well-known risks are impacting credit unions across the country. Many of these losses and their severity can be significantly minimized with proper loss controls.

**Concerning credit union loss patterns**

- **Account takeovers**  
Fraudsters have launched sophisticated social engineering attacks against members to scam them into providing their login credentials, including two-factor authentication passcodes.
- **Fraudulent checks clearing member accounts**  
The stolen mail problem has resulted in a significant increase in fraudulent checks clearing member accounts. Fraudsters steal members' issued checks and alter them (payee) or manufacture fraudulent checks using the info from members' legitimate checks.
- **Fraudulent deposits/U.S. Treasury checks**  
Fraudsters frequently social money mules to open accounts of credit unions to cash stolen or fraudulent Treasury checks. Fraudsters also open fraudulent business accounts in the name of the payees listed on stolen Treasury checks.
- **Interactive Teller Machine (ITM) fraud**  
Fraudsters are using the self-service feature to withdraw funds from member accounts – primarily using counterfeit debit cards. In some cases, deep insert skimmers were found on ITMs.
- **ATM jacking**  
These cases involve fraudsters installing malware via the ATM top hat, connecting a black box device, or through remote network attacks. Once installed, fraudsters issue a command to dispense cash immediately or an opportune time.
- **ATM smash 'n' grabs**  
A resurgence in ATM burglaries where criminals use a blow torch or other forced entry to open the ATM's money chest or steal it altogether.



**TruStage**  
 Risk & Compliance Solutions | Presentation

**Emerging risks outlook**

Rethinking protection in an era of uncertainty

Proprietary and confidential. Do not distribute.



0:00:00

# 2025 Risk Management Virtual Event Schedule

| Month     | Day | Topic   |
|-----------|-----|---|
| January   | 22  | Third-party & N <sup>th</sup> party cyber incidents |
| February  | 19  | Money mules & their schemes                         |
| March     | 19  | Lending landscape                                   |
| April     | 23  | Business continuity & incident planning             |
| May       | 21  | Disruptive technologies & risk trends               |
| June      | 18  | Employment practice risks                           |
| July      | 23  | Cyber threats & fraud                               |
| August    | 20  | ITMs & ATMs: a criminal's money chest               |
| September | 17  | Transaction fraud & scams                           |
| October   | 22  | Managing data privacy risks                         |
| November  | 19  | Business services & the risks that come with them   |
| December  | 10  | Emerging risks outlook: 2026                        |

**TruStage**

## 2025 virtual events

### Risk management

Stay ahead of the complex array of ever-changing risks, compliance issues, and industry regulations with our 2025 risk management virtual events. Each session is focused on emerging risks and loss trends impacting organizations just like yours. You'll gain actionable insights, proven guidance, and relevant resources that you can use.

**New in 2025... Cyber risks mini-series** – a 90-minute session held quarterly focused on sharing best practices and fundamental components related to preparing for, defending against, and responding to cyber & data threat trends.

**Register now at [www.trustage.com/bprc](http://www.trustage.com/bprc)**

**January 22**  
Third-party & n<sup>th</sup> party cyber incidents 90-minute cyber session featuring live Q&A

73% of total reported incidents involved compromises with a third-party service provider according to the NCUA. Unfortunately, vendor due diligence and contract safeguards mean nothing if third- and n<sup>th</sup> party data privacy and security requirements are an afterthought.

Join our expert panelists as they address how decisions regarding strategic partnerships with third-parties – and the vendors that they use – can extend the risk exposure and misuse of credit union or member's data.

**February 19**  
Money mules & their schemes

Money mules recruited in account takeover schemes and fraudulent deposit schemes (e.g., opening accounts at credit unions to cash fraudulent Treasury checks) are happening at record pace

Join TruStage™ risk consultants as they share ways to identify schemes and stop money mules and learn how to educate your members to minimize these scams.

**March 19**  
Risks & the lending landscape

Navigating the lending landscape is challenging. Considering the complexity of risks associated with fraud, vendor due diligence, internal controls, and regulatory compliance; there has never been a better time for credit unions to begin the strategic discussion to help you thrive in the current environment.

Join TruStage risk consultants as they share some of the changing lending dynamics related to fraud, vendor management, internal controls, and regulatory compliance.

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

Executive Vice President - \$3+ billion credit union

All events begin at 1:00 p.m. (Central). Register at [www.trustage.com/bprc](http://www.trustage.com/bprc)

**TruStage** Proprietary and confidential. Do not distribute. | 2

10010454-0924 © TruStage





# Thank you.

**Contact**

**[riskconsultant@trustage.com](mailto: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.