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 recruit money mules to open accounts at 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 jackpotting**
  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.

Top emerging risks

	Emerging risk	Probability	Severity	Primary control
1	Account takeovers	Frequent	Critical	Two-factor authentication
2	Fraudulent checks/deposits	Frequent	Critical	Employee training
3	ITMs/ATMs	Probable	Critical	Physical security
4	Human error/social engineering	Frequent	Marginal	Employee training
5	Vendor incidents	Occasional	Critical	Vendor oversight
6	Data privacy & protection	Occasional	Critical	Compliance program
7	Incident planning	Occasional	Marginal	Plan testing & preparedness
8	Loan fraud	Likely	Marginal	Employee training
9	Workplace safety	Remote	Negligible	Safety plan; employee training
10	Consumer protection	Occasional	Critical	Compliant processes

*Numbers indicate risk on chart not rank order

Other emerging risks on the radar

Considering that risks tend to rapidly emerge and evolve at any time, you must avoid becoming static. You need to identify and assess risks while ensuring controls are implemented and monitored on a continuous basis.

These additional emerging risks are also being closely monitored as we move into 2025:

- New account fraud
- Wire fraud
- Member scams
- Fraudulent instruction; Business email compromise
- 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.

Looking for additional insights?

- Access the **Business Protection Resource Center** (User ID & password required) for exclusive risk and compliance resources to learn more about these emerging risks and to assist with your loss control efforts.
- If you'd like to discuss these emerging risks in more detail, simply connect with a TruStage™ Risk Consultant at **riskconsultant@trustage.com** or at **800.637.2676**.