TruStage™

Let's Talk

emerging risks

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 and schemes.

To drive executive action on emerging risks, you typically try to limit the number of risks presented to senior management by providing a prioritized view. This approach shifts the emerging risk conversation from information-sharing to actionable decision-making.

Ensuring your organization and operational teams act on emerging risks, it is critical for you to provide a view that is prioritized based on specific potential consequences for the business.

However, the evolution of emerging risks is often uncertain because it can be rapid, random or both.

Emerging risks are often categorized

- **new** (recently introduced or unforeseen)
- **evolving** (impacting more functions and organizations as time goes on)
- **well-known** (repeat offenders with consistent frequency & severity)

However, no matter the placement, they can impact an organization's financial stability, disrupt business strategy, and impact your operations.

As the financial services industry evolves, so do the risks that you face. And, considering that risks tend to rapidly emerge and evolve at any time, you must avoid becoming static. You need to identify and assess risks – fraud, cybersecurity, operations, and compliance – while ensuring controls are implemented and monitored on a continuous basis.

CRITICAL LARGE LOSS PATTERNS

Six- and seven-figure losses over the last 18 months from relatively well-known risks are impacting many across the country; however, these losses and their severity can be minimized with proper loss controls.

- **Account takeovers**
  Fraudsters use sophisticated social engineering attacks against members to scam them into providing their login credentials, including two-factor authentication passcodes.
- **Fraudulent checks clearing member accounts**
  Stolen mail has resulted in a significant increase in fraudulent checks clearing member accounts. Fraudsters steal members' issued checks and alter them 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 checks, including Treasury checks. They also open fraudulent business accounts in the name of the payees listed on the checks.
- **Interactive Teller Machine (ITM) fraud**
  Fraudsters use 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.
- **ITM / 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 at an opportune time.
- **ITM / 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.

Check out www.trustage.com/emerging-risk for more details.

Emerging risk governance & planning

Effective risk management is more important than ever. You need to take all inputs, analyze them, identify the relevant risks and prioritize them. Then develop a plan to control the risks and enhance your strategy. Evaluating risks should be a continuous process as they can change quickly. It is not a set it and forget it process.

Financial institutions face new threats every day, yet very few executives believe their organization has processes in place to cope with that pace of change. Reputational impacts are being magnified. And the costs associated with risk mitigation keep rising—making it more difficult to quickly and cost-efficiently roll out new products.

Conventional approaches to risk management are being strained to the breaking point by multiple pressures. Probability, severity, and impact are cornerstones of the process but those shouldn't be the only lens used to evaluate risk. And that's because we tend to only focus on the immediate or near-term risks.

Merely focusing on near-term risks may prepare your decision makers for risks emerging in the next year or two. But what about the longer term of 3, 5 or 10 years out?

When you facilitate risk committee discussions, you should also consider discussing topics like trajectory and velocity of the risks. It's important for decision makers to understand how a specific risk is trending as well as speed of onset when contemplating where to invest resources and prioritize response efforts.

Probability

Anticipated
Possible
Unlikely
Likely
Unforeseen
Certain

Severity

Negligible
Marginal
Moderate
High
Critical
Catastrophic

Trajectory

Surging
Approaching
Departing
Consistent
Unpredictable

Velocity

Slow
Moderate
Aggravated
Rapid
Extreme

Impact

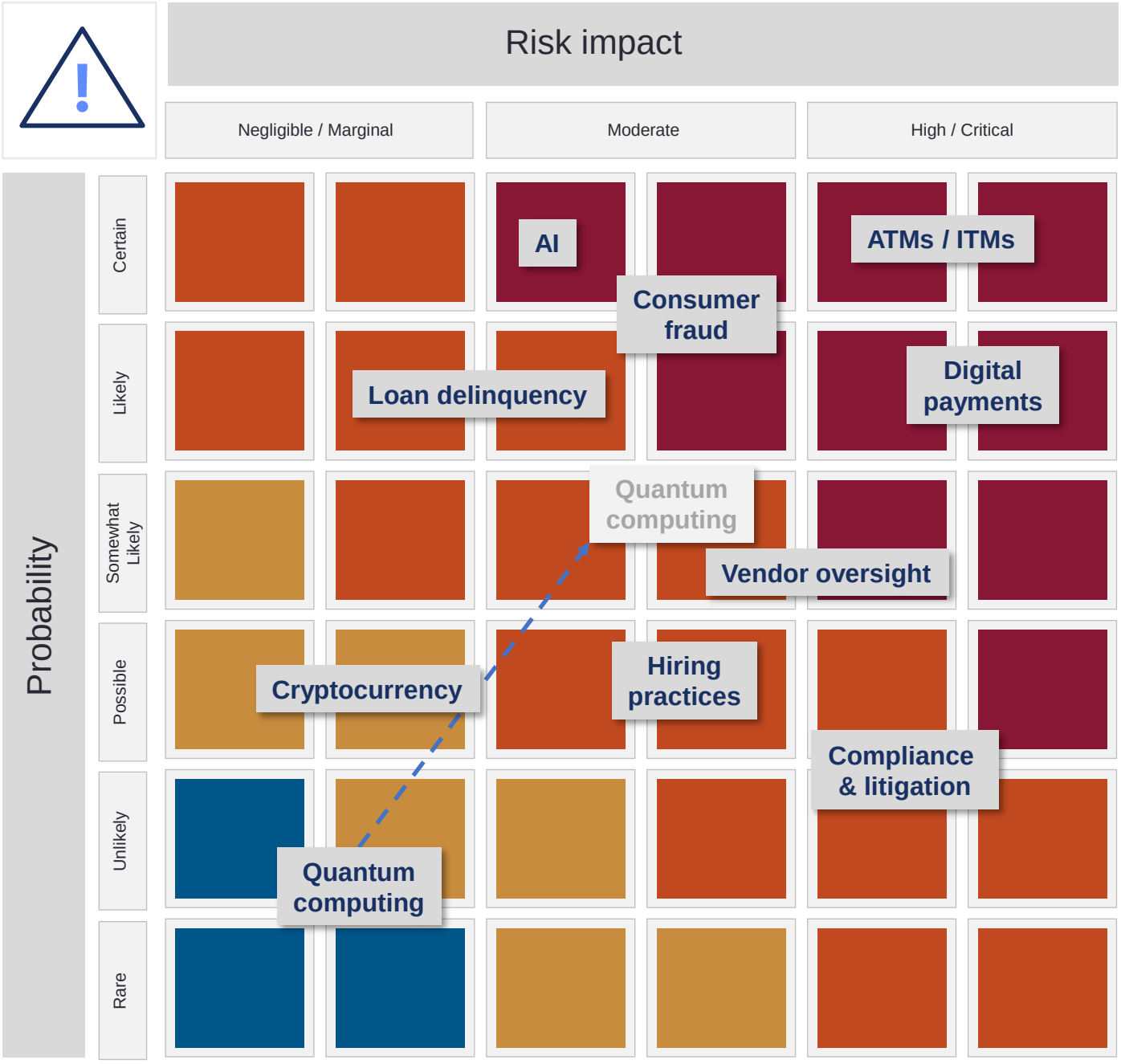
Operations
Employees
Reputation
Consumers
Community

Your readiness and resilience in the face of disruptive change and unexpected surprises brought on by risks is crucial. Having the ability to adjust and pivot could become the key differentiator between those organizations who are able to simply respond to changes in the landscape and those that are able to capitalize on opportunities that changes bring.

Emerging risks heat map matrix - 2026

In addition to some of the more well-known risks and loss trends related to fraudulent deposits, check fraud and account takeovers; some emerging risks require deeper review of key insights and strategies that can assist you in effectively managing them in 2026 and beyond.

By using a heat map, you can visually better understand the emerging risk concept and the factors that can shape your analysis and actions. The matrix includes colors to effectively convey which risks are of most and least concerning. The heat map information is designed to be a guide to address risk prioritization and provide a starting point for your risk mitigation and minimization strategies.



This overview is based upon losses, observed risk exposures, and other threats assessed, reviewed, and prioritized by TruStage™ Risk Consultants to formulate these high-level conclusions and loss control suggestions. You are encouraged to continuously review these and other emerging risks to determine the impact to your organization.

ATMs / ITMs

Background

Automated Teller Machines (ATMs) and Interactive Teller Machines (ITMs) are part of your members' digital culture and are a significant part of the branch of the future.

ATMs offer a significant convenience with direct access to cash transactions for both members and non-members alike. The convenience features offered with ITMs allow members to interact with a live teller on the screen, use the ITM as a traditional ATM, or take advantage of the self-service feature. However, fraudsters and criminals also find ATMs and ITMs useful and convenient to gain access to money if the proper controls and security are not in place.

A growing number of risks include:

- physical security as criminals use aggressive smash & grab attacks to gain access to cash canisters.
- employee safety concerns related to practices and procedures involving currency transportation, fulfillment, and service.
- fraud, scams & malware connected to card skimming, shimming, jackpotting, and malware used to manipulate system controls.
- member safety resulting from robbery, physical attacks, and other safety incidents.

ITMs are also quite vulnerable to losses related to fraudulent checks, deposits and account takeovers. Because these ITM transactions are often run through core systems; they often have larger withdrawal limits and access to several accounts held by the member. In addition, these fraudulent transactions are often completed during off hours.

Loss control roadmap

Button up machine security.
Fraudsters take advantage of weak security protocols and often attack the physical terminal by installing malware through the machine's top hat.

Security devices such as heat sensors, seismic/tilt sensors, bollards, barrier systems, strobe lights, and alarms are encouraged.

Implement key controls.
Work with service providers to keep your machines, operating system and software properly set-up and up-to-date.

Limit certain self-service transactions. Blocking fallback transactions for the self-service feature is a critical control to adopt.

Inspect your machines regularly.
Machine tampering and fraudulent transactions are often completed during off hours – especially during late night hours, weekends and holidays – to help fraudsters remain relatively unnoticed.

Use an inspection checklist to look for tampering, foreign devices, and security risks daily.

Educate your members.
Sophisticated social engineering attacks are used to scam members into providing their login credentials, including two-factor authentication passcodes.

Encourage them to report any signs of tampering or unusual devices found on ATM/ITM terminals.

Related resources

- ATM safeguards risk overview & inspection checklist
- ITM risk overview

Risk outlook: ATMs / ITMs

The functionality of ATMs and now ITMs has evolved over time; yet these machines remain prime targets for criminals and fraudsters looking to score quick cash and access to accounts. And, with more than half million machines estimated nationwide, ATMs and ITMs provide ample targets.

With more machines expected and the need for greater cash storage, more access to mobile units, and new ATM/ITM self-service functionalities being used to serve members and non-members; it should be anticipated that fraud and physical attacks will continue to remain constant and evolve as bad actors find new ways to attack them.

Artificial intelligence (AI)

Background

Given the rapid advancements and growing interests in AI across a diverse segment of industries, many credit union executives are looking for ways to embrace the technology to streamline processes, enhance customer experiences, and optimize operations.

AI adoption by credit unions has already grown significantly, moving from early, tentative steps to a more strategic integration.

Key AI application already being used include:

- Enhanced lending involving underwriting and automated decisioning
- Enriched member experience and servicing with the integration of increased personalization and chat bots and/or voice assistants
- Improved fraud detection and cyber risk prevention
- Managed employee life cycle from recruitment, hiring, performance management and employee development

Vendors have also begun to use AI within the products and services that they provide to credit unions. It is critical for you to be aware of security, privacy, and ethical practices as it relates to how AI is being used by those third parties.

Perhaps no recent technological innovation like AI has transformed so much, including itself, so quickly. Unfortunately, AI is not perfect. There is more clarity still to be uncovered regarding risks including privacy and regulatory expectations. In addition, there is continued threat actor use and evolution of AI usage in scams, fraud, and other threats.

Loss control roadmap

Hire AI skilled leaders.
Make the strategic shift by hiring successful AI leaders with demonstrable skills with a blend of technical acumen and human leadership qualities.

Build a solid AI framework and governance.
Having a proactive AI governance strategy will be vital for your organization. You must understand the risks and prioritize ethical AI principles, including fairness, transparency, and accountability.

Consider how AI compliments your solutions.
When planning for AI, it is critical that you consider the value and efficiencies along with defining your risk appetite. Having a method to assess business need and risk prior to introducing or allowing AI use will be helpful in the short term and long run.

Develop acceptable use policies.
Establish boundaries for AI tools that includes data collection guidelines, privacy and compliance requirements used to query or converse with the AI tool. Prioritize and share with your employees the use cases you have identified and explain how you (and they can) plan to leverage the AI technology.

Manage AI risk, bias and be compliant.
Fraudsters are now deploying AI to enhance fraudulent scam activity and create deepfakes to increase social engineering scam effectiveness. Malicious actors have also taken to developing their own LLMs, such as WormGPT and FraudGPT, and advertise them for sale in hacker forums.

Related resources

- Artificial intelligence risk overview
- Deepfake risk overview

Risk outlook: AI

While it is unclear how rapidly AI capabilities will progress or how quickly risks will grow, it is widely expected that the AI transformation will present some significant challenges and emerging risks. AI integration is still in the early days; know that emerging risks involving AI are real and will continue to evolve.

Unfortunately, AI risks could balloon before they become more stable with potential privacy violations, algorithmic bias, misinformation, as well as enhanced security threats like data poisoning, deepfakes, and sophisticated cyberattacks. Potential long-term and current risks could be exacerbated with the integration of AI systems especially those without the necessary oversight and lack of accountability.

Consumer fraud

Background

Consumer-targeted fraud continues to grow with the deceptive practices and tools criminals have access to today. Unfortunately, these fraudsters are getting better at tricking consumers/members into giving up money, personal information or access to accounts.

The focus is to prey on the human nature to trust, play with emotions, and introduce a sense of need or urgency. Often, they are recruited as money mules to assist fraudsters - knowingly or unknowingly - launder ill-gotten funds.

Consumer-targeted fraud accounts for billions of dollars lost and can erode the trust your members have in your organization.

Consumer-targeted fraud continues to grow with:

- Better and easier-to-access technology to add to the fraudster's arsenal – inflicting malware, deepfakes, and phishing campaigns
- Enhanced social engineering and SMiShing tactics. In addition, fraudulent business models outside of the U.S. where scammers build relationships with targets to invest – most often with crypto (aka "pig butchering")
- Breaches outside of your organizations provide fraudsters with PII and other key information
- Lack of education on latest scams and schemes

Related resources

- Fraud & scams member risk overview
- Elder financial abuse risk overview
- Employee interactive training module: When Members Become Victims

Loss control roadmap

Educate all staff on scams on an ongoing basis.
Fraud and scams are often hard to detect at a quick glance; however, by being aware of common red flags, your employees can be better prepared to help and consult with members.

Raise fraud awareness with members.
Provide members with proactive tips and actions to ensure personal and sensitive information is not compromised. Encourage them to remain vigilant and be suspicious of unsolicited emails, texts, and phone calls. Fraudsters will disguise their identity while retrieving confidential member information.

Invest in fraud detection and monitoring.
Consider deploying a more secure form of two-factor authentication, such as a token or push notifications to a dedicated app residing on the member's device. In addition, a real-time fraud monitoring solution with behavioral analytics that leverages the use of artificial intelligence and machine learning can assist in minimizing risks

Promote a Trusted Contact Program.
Implementing a trusted contact program can assist you when a member is convinced that they are doing the right thing. The trusted contact will not have transaction capability unless they are a joint owner; however, the contact is someone to share concerns about possible financial exploitation or the account owner's capacity to manage their account.

Incorporate monetary transaction limits.
Ensure transaction limits – single monetary transaction and daily limit – for all payment types offered are reasonable.

Risk outlook: Consumer-targeted fraud

Each year, fraudsters find new ways to trick people out of money. While some scams involve new approaches, many have been around for decades. No matter the approach, The scams look to catch your members off-guard and to dupe them into making security mistakes or giving away sensitive information and money.

Fraud risk is escalating on all fronts, and it doesn't appear to be slowing down. Smarter technology will only make threats and scams even more difficult to detect. Common scams like romance scams, fake tech support, and government imposters that involve impersonation will grow in sophistication and target the weakest link: humans of all generations.

Digital payments

Background

Financial technology has propelled the speed at which payments are made and significantly increased the reach of digital payments. Digital payments typically occur in real-time and payment services are generally free to use.

Digital payment innovations allow financial institutions to remain competitive and improve the payment experience for their members. The total amount of digital payments globally in 2024 is estimated to be USD $18.7 trillion (Worldpay 10th Global Payments Report).

Digital payments include any transaction where funds are transferred electronically via online, mobile, or connected-device platforms.

- Mobile wallets
- Person-to-person (P2P)
- Account-to-account (A2A)
- Buy now, Pay later (BNPL)
- Card on file/preloaded funds

The main digital payment risks involve fraud, identity theft, account takeovers, security vulnerabilities, and technical issues like transaction errors and payment system failures. There are also potential risks of losing funds due to unauthorized transactions and difficulty in resolving disputes and chargebacks.

50% of credit union members use a digital wallet at least a few times per month, up from 27% in 2022.

2024 Eye on Payments Report, Velera

Loss control roadmap

Know how to identify a digital wallet transaction.
As the volume of digital transactions grows, so does the need for you to know how the flow of a digital wallet transaction works.

Understand enrollment, tokenization, authorization, and dispute handling.
Understanding the nuances of important concepts with digital payments is key to enhance security, improve the user experience, drive growth for payments and reduce complexity with integration.

Set fraud rules.
Securing digital payment methods is crucial to maintaining consumer trust and protecting sensitive data. As digital payments evolve, the need for effective controls grows, requiring a multi-layered approach to minimize risks.

Real-time fraud monitoring.
Continuous monitoring of payment systems helps detect suspicious activity early. Advanced threat detection technologies, like AI and machine learning, can identify anomalies in real-time, allowing for faster response to potential threats.

Stay focused on fraud & scam risks.
Educating member users on proven practices, such as recognizing fraud, scams & phishing attempts and creating strong passwords, plays a crucial role in digital payment security.

Related resources

- Provisioning & tokenization of mobile wallets checklist
- Mobile payments risk overview

Risk outlook: Digital payments

Digital payments have surged in popularity and are playing an increasing role in today's financial landscape as consumers embrace the convenience of cashless transactions. The significant increase in the use of digital payments has also increased the potential for financial crime risks, particularly fraud.

Behind the scenes, bad actors are keeping up with advances, often developing new strategies to exploit digital payment products and services and take advantage of vulnerabilities and weaknesses within your organizations' framework of safeguards. In today's digital-first world, securing payment systems is more important than ever.

Vendor oversight

Background

There is a growing reliance on working with third-party service and product providers to fulfill operational and member-facing needs. Third-party vendors play an important role as you strive to become more competitive and expand services.

However, vendor management and oversight is no longer a check the box component of compliance; it has evolved into an ongoing operation with expectations that the vendor will be continually vetted, monitored, evaluated, and assessed throughout the course of the relationship.

As financial services grows more interconnected, complex, and specialized, it's increasingly common for third-party vendors to rely on their own set of subcontractors or fourth parties.

Unfortunately, vendor due diligence and contract safeguards mean nothing if third-party data privacy and security requirements are an afterthought. Every outsourced relationship is unique, and there may be varying degrees of complexity associated with not only each vendor relationship but also the specific needs of the credit union.

Supply chain cyberattacks can cripple networks and jeopardize critical aspects of your organization's operation. Incident response plans must emphasize speed and flexibility, so you are able to quickly adapt to rapid change.

You can outsource the service; however, you still own the responsibility of the critical business practice.

Loss control roadmap

Build a roadmap.
Provide a systematic, ongoing process of analyzing and evaluating strategies, products or operations as the driver of vendor oversight. Be sure roles, responsibilities and expectations are clearly defined.

Know your vendors and set expectations.
Develop a thorough understanding of what the relationship will accomplish, and why it is important. Make vetting and ongoing monitoring a critical component of your roadmap. If your third-party vendors are entrusted with your credit union's member data, it is just as important as how you treat it yourself

Understand risk by asking the right questions.
As cyber attacks grow in frequency and severity, so do the obligations to understand the third-party and nth party risks in all facets of its relationship.

Establish processes to evaluate and manage third-party risks before entering, during, and even after the relationship ends. Ask critical questions and have open discussions - your vendor's responses can help you feel confident with their security, preparedness, privacy and ethical practices.

Develop and test your incident response plans.
While there is no one correct way to develop and test your incident response plans; it is important to continuously improve the plan by incorporating lessons learned.

Related resources

- Vendor management risk overview
- Critical vendor questions risk overview
- Incident response tabletop & discussion guide

Risk outlook: Vendor oversight

In today's complex business environment, vendors play a key role in your success. Vendor risk is an emerging area of significant focus, especially if that third party – or their vendors - plays a critical role in the delivery of products or services to your financial organization or members.

Unfortunately, third-party vendor losses – specifically cyber attacks - continue to grow in frequency and severity. These supply chain incidents can impact multiple organizations at a time. And, the disruption and costs to identify and resolve these incidents – along with the operational downtime and resource impact for your organization - can be staggering.

Cryptocurrency (Stablecoins)

Background

The Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act was signed into law on July 18, 2025, creating a federal regulatory framework for payment stablecoins issuers.

In general, there are three types of entities which can issue payment stablecoins under the GENIUS Act:

1. subsidiaries of insured depository institutions
2. nonbanks approved by the OCC
3. state-chartered companies regulated by state entities.

Federal credit unions are not allowed to hold custody of cryptocurrency; however, federally insured state-chartered credit unions have the authority to serve as a custodian subject to state law.

Some CUSOs are offering cryptocurrency custodial services with some credit unions participating as an investor or partner.

Reasons for offering cryptocurrency custody include:

- As digital assets become more mainstream, credit unions can lose members if they don't offer the services they need.
- Banks have been able to offer crypto custody services since 2021; credit unions look to adapt to remain competitive in the evolving landscape.
- Offering crypto custody can open new, high-margin services and revenue streams.
- Use established reputation to provide secure and reliable alternative to centralized exchanges.
- Offer members a secure way to store their digital assets, reducing the risk of theft or loss that comes with self-custody or unregulated platforms.

Primary risk impact

- Theft of investors' cryptocurrency has been well-publicized.
- The likelihood of account takeovers of members' cryptocurrency accounts/wallets is unknown. However, there is the potential for large losses considering today's social engineering attacks against members to obtain login credentials.
  - Account takeovers as the result of the SIM swapping scam allowing fraudsters to intercept 2-factor authentication passcodes.
  - Account takeovers as the result of phishing scams to capture login credentials and 2-factor authentication passcodes.

Loss control roadmap

Carefully assess risks.
Perform a risk assessment and conduct due diligence on 3rd party providers of cryptocurrency custodial services. It is expected that you have a thorough understanding of the services and associated risks.

Strong-layered security controls.
Ensure adequate risk management and strong layered security controls are in place for accessing members' cryptocurrency accounts / wallets.

Keep a watchful eye.
The next step is for NCUA and other regulatory agencies to issue a joint rulemaking to implement the provisions of the GENIUS Act. Stay focused on changing regulations, compliance and market volatility. It is important to adhere to strict regulations including anti-money laundering, verifying consumer identities, and monitoring for suspicious activities.

Risk outlook: Cryptocurrency (Stablecoins)

Stablecoins represent a new kind of deposit that has the potential to pull balances away from credit unions. The GENIUS Act sets the stage to allow entities of all types to issue their own stablecoin programs. It is critical to navigate the complexities of crypto-asset safekeeping with diligence and a significant risk management focus.

Many credit unions that are taking a wait and see approach and will not offer cryptocurrency custodial services through a third-party service provider this early; therefore, it is not anticipated that account takeovers of members' crypto accounts/wallets will occur in 2026. However, as more credit unions offer services, it can be expected that losses would escalate as bad actors also converge on the new offering.

Hiring practices

Background

Today's job market and a lack of a seamless succession plan can require you to make quick hiring decisions. Add in that four or five different generations with different backgrounds, life experiences, and priorities are employed at your organization.

The impact of quick decisions that are wrong can lead to sunk costs and expenses related to lost productivity, training, recruitment, and even fraudulent activity. Add-in imposters now posing as legitimate remote candidates using stolen identities, submitting AI-generated resumes, and using deepfake technology to conduct interviews, it can be difficult to know who you're potentially hiring.

Issues like limited experienced candidates, an aging workforce, immediate transition need, remote work, and fraud can easily get in the way and encourage hiring managers to side-step critical hiring practices.

In addition, hiring assessments can be a slippery slope for employers, especially when they rule out protected employees and create disparate impact. And, if you're using AI…have you tested the predictive validity – meaning that it doesn't have discriminatory impact on certain protected classes and accurately measures knowledge, skills and abilities that are directly relevant to the job.

Related resources

- Employment Practices Risk Management website
- HR & Succession plans risk overview
- Background & reference checks risk overview

Loss control roadmap

Have a plan.
When hiring employees, as the employer, you have some risks, rights, and responsibilities to that employee and to all future employees. However, new laws and responsibilities have made it clear that treating all employees fairly and the same way is important. Ensure you have a succession and human resources plan – obey the rules, policies and deal honestly.

Develop and maintain clear job descriptions.
Written job descriptions are more important than ever and should be reviewed at least annually and whenever there is an opening for that position. Any physical requirements, essential job functions and workplace arrangements (e.g., remote work) should be clearly communicated. Always be sure you are following the employment laws of the states in which your employees reside.

Check the background.
Conducting a through background and reference check on employees is essential. Screening may include verifications of past employers, credit checks, criminal background, educational background & licensing, drug testing, and personal & professional references.

You should seek the guidance of an attorney specializing in employment law before making a decision whether or not to use social media for applicant screening.

Verification against the TruStage™ exclusive Bondability claims database is also an important step to identify potentially bad hires.

Risk outlook: Hiring practices

Ultimately, making strong hiring decisions protects the company, its personnel, and its resources. Risks related to hiring practices include legal liabilities from discrimination, costs from high employee turnover, and poor performance from inadequate hiring practices like rushing the process or ignoring cultural fit. Effective recruitment and hiring practices mitigate these risks through structured interviews, thorough background checks, clear job descriptions, and ensuring legal compliance.

The phenomenon of shifting jobs – often within six months of the initial hire date – is a reality. Misrepresentations made during the hiring process compared to the reality of the responsibilities of the position can lead to more turnover and more opportunity for negative aspects to occur.

Compliance & litigation

Background

Compliance risk occurs, primarily, from failure to comply with federal, state and local laws and regulations. And, non-compliance can result in regulatory fines, civil money penalties, restitution and damage to reputation.

The potential also exists for class-action litigation from attorneys that seek to exploit a credit union's non-compliance with consumer protection and data privacy laws.

The scope of compliance appears to be much broader and its impact on organizations is far greater than ever before. Recent litigation trends include:

- Website accessibility
- Session replay, wiretapping, digital tracking & web analytics (Pixels)
- UDAAP
- Defective post-repossession (collection) letters
- Telephone Consumer Protection Act
- Overdraft/NSF fees
- Fair lending
- Data privacy
- Employment-related litigation such as retaliation and discrimination

Compliance risk is an ongoing concern and establishing compliant operations can be challenging. It often increases the cost of service and sometimes makes the delivery of a great consumer experience more difficult.

Loss control roadmap

Remain focused.
You should remain strategically focused on evolving threats and new rules, such as those related to data privacy and artificial intelligence.

Formalize a governance program.
Leverage technology for automation and efficiency. You should have a formalized written data and compliance governance program in place to assist as well as to provide to examiners, regulators and auditors.

Train employees.
All employees should be knowledgeable, empowered and accountable for regulatory compliance specific to their role. For example, lending staff should be well versed on fair lending compliance, including Equal Credit Opportunity Act (ECOA), the Fair Housing Act (FHA) and the Home Mortgage Disclosure Act (HMDA).

Ensure third-parties are adequate.
Establishing processes to evaluate, re-evaluate and manage associated vendor risks before entering, during, and even after the vendor relationship ends. Remember, vendor risk management is an ongoing process. Knowing that your vendor is making compliance a priority and that they are committed to identifying and remedying problems is critical.

Related resources

- Emerging Risk Outlook: Compliance & litigation
- Data privacy, protection & governance risk overview
- Lending risks outlook risk overview

Risk outlook: Compliance & litigation

Regulatory risk is subject to change based on the political climate and from administration to administration. While the current administration has more of a hands-off approach, the underlying regulations remain relevant and subject to enforcement – particularly at the state level. In addition, predatory attorneys seemingly continue to look for regulatory non-compliance as a basis for class-action litigation – as seen with the recent pixels tracking and multi-plaintiff class action lawsuits by customers whose PII was accessed by unauthorized third parties as a result of a breach.

While the loss frequency is a bit unknown at this point, the risk should be ongoing concern with the impact for severe losses remaining.

Quantum computing

Background

Developments in quantum computing could bring beneficial improvements along with potential challenges and risks.

Quantum computing uses the principles of quantum mechanics to process information. Quantum computers process data using quantum bits or "qubits" using principles of superposition and entanglement to perform many calculations simultaneously, at unprecedented speeds.

With its immense processing power, quantum technology can analyze vast and complex transaction datasets almost instantly – even spotting hidden patterns that classical computers might miss in certain tasks or functions. In financial services, it could be used in:

- Enterprise risk management
- Cybersecurity & fraud management
- Retail banking
- Payments
- Asset/Wealth management
- Investment banking
- Operations & finance
- Lending and loan processing

However, not all is good news as it will likely pose threats to secure web traffic, digital contracts, digital signatures, email authentication, phishing protection, cryptocurrencies, and more. It is already time to prepare for these risks. In fact, encrypted data can already be stolen and stored until quantum technology is sufficiently advanced to break encryption ('harvest now, decrypt later').

Loss control roadmap

Don't wait. Build a research & development roadmap to actively explore its potential.

- Identify critical systems reliant on encryption, including digital signatures, encrypted cloud data, VPNs, and key exchanges.
- Incorporate quantum readiness into your vendor vetting – similar to approaches taken for the use of artificial intelligence.
- Re-encrypt long-term confidential and sensitive data with quantum-resistant algorithms.
- Integrate quantum-resistant algorithms alongside current encryption methods to ensure a smooth transition.
- Stay up-to-date with NIST's standards and recommendations. Explore compliance and legal obligations, including polices that may be needed for compliance and security purposes.
- Collaborate with peer organizations, technology providers and partners to build knowledge and identify solutions.
- Plan how to handle talent management and recruiting. Quantum computing requires a proficiency in quantum information science — a subject area with a substantial skills shortage.

Related resources

- Quantum computing risk overview
- Disruptive technologies risk overview
- Emerging Risk Outlook: Disruptive technologies

Risk outlook: Quantum computing

While widespread quantum computing is on the horizon, many financial institutions are already actively exploring its potential. Some organizations are in early stages of investing, researching, and preparing algorithm developments that will be ready to leverage this technology once it matures.

Today's risks appear to continue to be low as most monitor and research developments and challenges. However, the implementation and advancement of quantum computing technologies in the financial services industry could erupt. For those that have not invested in research and development, the risks generated from competition and your organization's unpreparedness could become significant very quickly.

Loan delinquency

Background

Delinquent loans continue to be on the rise at financial institutions across the United States.

A September report from J.D. Power found that more consumers are falling behind on their car payments, with wages stagnating and unemployment ticking higher. The percentage of new-car buyers with credit scores below 650 was nearly 14% in September, the highest for the comparable period since 2016. At the same time, the portion of subprime auto loans that are 60 days or more overdue on their payments hit a record of more than 6% this year, according to Fitch Ratings.

It appears that some borrowers may have stretched budgets to afford a higher price of the asset, as well as a higher payment because of the interest rate.

While more delinquencies can lead to collections and repossessions, three significant risks that should be on your radar are:

- Improper collection efforts and communications
- Damaged collateral impacting recovery value
- Purchasing and maintaining proper insurance

While, in theory, only the misbehaving members are the ones that supposedly fail to maintain proper insurance and uphold their collateral value as expected; unfortunately, that just isn't reality.

Related resources

- Lending risks outlook risk overview
- Collections risk overview
- Collection letter risk overview

Loss control roadmap

Protect your interest in collateral.
Consider options to ensure your members are actively protecting collateral as identified in the loan agreement. While there is usually only a small percentage of borrowers who either do not, cannot, or simply refuse to protect your interest in collateral; this leaves lenders like you at risk to potential loss if you end up repossessing damaged collateral.

- A **blanket policy** that protects your entire portfolio
- A **blanket vendor single interest policy** where you can pass the cost to your borrower and eliminate ongoing member communications.
- An **immediate issue program** that allows you to decide if you will place insurance and which member communications you send.
- **Full tracking option** that follows-up on insurance requirements and places insurance to protect your interest in collateral. Tracking the status of insurance on collateralized loans can provide a critical roadmap for risk, indicating which loans are not insured or at risk of not being insured.

Reset collection strategies.
Adjust focus primarily to high-risk and high priority members in the near term. Implement a consultative collections strategy that implements specific treatment strategies for members – such as loan restructuring with deferred payments, reduced interest rates, fee waivers, and loan extensions.

Ensure compliance.
Review policies and procedures to help ensure that loan and collections staff are aligned with your expectations – steering clear of litigation such as TCPA and deficiencies in collection letters.

Risk outlook: Loan delinquency

Metrics such as delinquency ratios and loan loss forecasting play a crucial role in identifying potential risks and implementing appropriate risk mitigation strategies for credit unions. Portfolio management is a key element of lending that shouldn't be taken for granted.

Fluctuating economic cycles can generally result in changes in credit worthiness. Many affected borrowers never imagined that they would be unable to pay their debts or properly maintain collateral. For some organizations, a wave of nonperforming exposures may appear and must be addressed in new ways. Minimizing losses by implementing socially responsible collections may be needed.

Other emerging risks on the radar

While everyone has its own unique risk footprint, this Emerging Risks Outlook introduces risks and trends that most likely should be on your 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 and throughout 2026:

- New account fraud; wire fraud; & loan fraud
- Fraudulent instruction; business email compromise
- Ransomware
- Internal controls & insider fraud
- Office safety; workplace violence
- Business continuity; disaster preparedness
- Employee retaliation; discrimination
- Real-time payments
- Data privacy & protection
- Social engineering & phishing

Keeping ahead of the complex array of ever-changing risks, litigation trends, and compliance issues that are impacting credit unions requires keen awareness, effective preparation and loss control scrutiny.

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 resources (including those linked in this document) within 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.
- Check out the **TruStage 2026 Risk Management Virtual Events** – including quarterly **Emerging Risks & Trending Losses office hours** sessions.
- 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**.