2020 eBook Series

Rise Above Your Risk

Emerging Risks Outlook

Risk & Compliance Solutions
800.637.2676
RiskConsultant@cunamutual.com

CUNA MUTUAL GROUP

Emerging Risks
on the radar

Risk	Description
Synthetic Identity Fraud	The foundation of a synthetic identity is personally identifiable information along with a compromised SSN that acts as the essential linchpin to build a believable credit record
Mergers & Acquisitions	M&A can be a healthy strategy to increase member base, penetrate new markets and acquire new products and technology. However, every aspect of the transaction must be considered before proceeding.
Digital Lending	Digital platforms can employ nontraditional approaches including collecting and decisioning on data sources which can lead to regulatory or compliance issues.
Cannabis Impact	The legalization of cannabis across the country presents uncharted territory for many credit union loan and deposit operations, along with human resources departments.
Member Authentication	Fraudsters continue to challenge credit unions with social engineering fraud tactics and by exploiting weak authentication methods connected to online member enrollment.
Talent Management	The principle step in nurturing a diverse and inclusive workforce should be the development of a well-thought out talent acquisition and management strategy.
Business Resiliency	The investment in your branches and day-to-day operations is often only as good as your people, situational awareness, and the preparedness levels for your operations to survive and thrive.
Governing Cyber Risk	Often considered a backend IT process, cybersecurity is actually a governance strategy that the C-suite to every staff member in your organization should support and follow.
Next Generation Defenses	New technologies like Artificial Intelligence and Machine Learning are emerging to bolster defenses; however, credit unions are still looking for ways to successfully integrate.
Employee / Workplace Safety	Unfortunate events involving workplace safety and security – from slip, trips, & falls to active assailant situations – forces organizations to prepare for hazards of all types.

Emerging Risk

Emerging Risk is a systemic issue or business function that either has not previously been identified or is unforeseen, has recently become more aggravated or evolving more broadly, or has been identified and hung around for an extended period of time.

In this resource, **Emerging Risks Outlook**, CUNA Mutual Group Risk Consultants and insurance specialists share the risks, threats, and challenges they see looming on the 2020 horizon — from operational risks, change initiatives, external factors.

It is critical that your credit union is monitoring emerging risks and is also developing actionable controls based on the risk impact, likelihood, velocity and time horizon.

Learn more by reaching out to a CUNA Mutual Group Risk & Compliance Consultant:

- **800.637.2676**
- **riskconsultant@cunamutual.com**
- **Protection Resource Center** @ cunamutual.com

Rise Above Your Risk with Confident Decisions

When considering an emerging risk framework, you must be sure that you're not doing something that could put your long-term viability in jeopardy. Ask yourself if there's a new level of scrutiny that your organization now needs to apply. Because, as you grow in assets, geographically, employee size, functions, processes, and within your membership base…more eyes are on you. Those eyes can include competitors, regulatory agencies, consumers, your current and potential employees, and fraudsters - all paying attention to your next moves or possibly your lack of thereof. And, remember your emerging risk framework should continue to evolve.

Risk Universe

Risk management was often described as "the department that says no." Today's risk management is characterized more as the function that enables successful execution with the risk universe in mind.

Technology & Next Gen Vulnerabilities

Evaluate the potential for technology system failures and innovation lag.

Explore the organization's & third-party relationships' infrastructure, access controls, and data privacy protections.

Compliance & Litigation

Understand risks that result from an increasingly complex regulatory and compliance environment.

Monitor developments in class action litigation and implement strategic guidance and tactics to minimize potential loss.

Payments, Fraud & Scams

Address vulnerabilities to both external and internal fraud and scams.

Assist the organization in developing a plan to curb risks and implement appropriate fraud risk detection and response.

Operations, Security & Employees

Evaluate losses that result from inadequate or failing processes, control, people, or systems.

Ensure supply chain and vendor relationships are monitored / aligned with the risk appetite.

Synthetic Identity Fraud

Easy to create.
Real identities are permanent, but fake identities can be created, used and then discarded in as little as a few minutes.

A predominant tactic for fraudsters

$355 million in outstanding credit card balances are owed by people who are suspected did not exist in 2017 according to TransUnion.

Synthetic identities are created by applying for credit using a combination of real and fake, or sometimes entirely fake, information. While these applications are typically rejected because the credit bureau cannot match the name in its records; the simple act of applying for credit automatically creates a credit file at the bureau in the name of the synthetic identity. This allows the fraudster to set up accounts in this name and begin to build credit. And, the fact that the credit file looks similar to others who beginning to build their credit record—that is, there is limited or no credit history — it makes the scam nearly impossible to detect.

The foundation of a synthetic identity is personally identifiable information along with a compromised Social Security number that acts as the essential linchpin. In order to avoid detection, fraudsters prefer to use Social Security numbers of those least likely to use credit**, typically children, the elderly or the homeless**.

This synthetic identity may be comprised of one person's name, a second person's Social Security number, a third person's physical address, and some fabricated information such as a fictitious place of employment. This appearance of an identity — made from combining just enough real data and fake data — allows fraudsters to apply for credit, make major purchases, and establish a convincing financial history over time. When the credit lines are maximized, payments cease and the fraudsters walk-away leaving lenders holding the bag.

Synthetic identity fraud is the fastest-growing type of financial crime in the U.S. and is estimated to account for 10-15 percent of charge-offs in a typical unsecured lending portfolio.

Source: Fighting back against synthetic identity fraud. January 2019. McKinsey & Company

Without an efficient way of uncovering synthetic identity fraud, credit unions should consider utilizing technology to defend against the innovations of synthetic identity fraudsters. **Data analytics** is considered the future of online member authentication. Leveraging third-party data can be a valuable tool. Fraudsters often fall short in failing to consider that real people have real histories found in physical and digital databases. An individual's history has depth, includes years of data, and is hard to fake. There should be consistency from database to database. Synthetic identities tend to be inconsistent, because any real information used in the identity creation is likely from multiple individuals.

Machine learning typically has the capability of sorting through the vast amounts of third-party data to gauge whether the application information submitted by an applicant matches that of a real person; thereby, weeding out those likely to be using a synthetic identity. This will provide your organization with a smaller group or subset of applicants to focus more in-depth identity checks without inconveniencing legitimate members.

Nonprofit organizations within field of memberships are especially attractive to fraudsters pursuing synthetic identity fraud. They only have to join the nonprofit organization, or make a small contribution to a charitable organization, to qualify for credit union membership.

Action Steps To Stem Synthetic Identity Fraud

While data analytics is the future of online member authentication; some traditional methods to defend against synthetic identity fraud include:

- Monitor for any Social Security number that matches a different consumer while no credit file is available for the requested applicant.
- Screen for credit files where the name and address of the applicant match, but the Social Security number matches a different consumer and vice versa.
- Look for inconsistencies in information provided on the loan application and verified by third party sources, i.e. Credit Reporting Agencies (CRAs).
- Require different forms of authentication such as verifying requestors via other means of communication. If a request is made by email, for example, then make a phone call to a previously established number to verify the transaction.

Conclusion

Synthetic identities are one of the more challenging fraud patterns to detect and prevent because the fraudsters' methods, behaviors, and outcomes are so diverse. It is expected that fraudsters will continue to commit this type of crime due to the difficulty in detection with increased digitization and high payoffs for fraudsters.

TRENDING

Websites Deliver Realistic, Instant Full Identities

One website, Elfqrin, provides tutorials and programming code to create a new virtual disposable identity instantly. The website randomly generates a realistic identity with some real and some fake information which can be used for a variety of purposes – one of which is fraud.

Most problematic is that the identity information combines real data, such as social security numbers and drivers license information, that closely matches the location of the fake identity. This can definitely fool lenders that do not have proper controls and authentication measures in place.

While the website does not condone fraud and advises it is for games, novels or avatars; unfortunately, fraudsters have disregarded this warning.

Another popular website purportedly used by fraudsters is SSN Validator which provides a full check on the validity of the social security number, the date and state it was issued and a check on the Death Master file.

Mergers & Acquisitions

A reality in the financial services landscape.
Many leaders are rightly concerned about how a merger would affect their operations, their employees, and their members.

Never a good time for surprises

Mergers and acquisitions (M&A) can elicit strong emotions. For some, it is viewed as an exciting opportunity for growth. For others, including Board of Directors, employees, members, sponsor groups, it can be feared as a loss of control, quality, and culture. While M&A may make sound financial sense, credit unions can run the risk of losing a stake in the communities they serve in their pursuit to stay competitive. This can be a significant breakdown. In order to pursue a well-structured, strategic M&A plan, you'll want to mitigate potential issues and challenges.

DUE DILIGENCE. Even if you know your merger partner well, you have a fiduciary responsibility to members to dig deeper into the most impactful areas including financial, legal, products, and human resources. The ultimate goal is to understand how the entities would best be combined into one credit union, including; looking for a cultural fit that is aligned with your business goals, and is in the best interest of your current and acquired members. To accomplish this goal:

- Address the tough, deal-breaking questions first, before a commitment between the two entities is made
- Review at least three years financial statements to identify trends
- Review loan portfolios, loan files, underwriting standards, collection practices. charged-off loans, delinquent loans, expenses, department budgets, investment programs, investment portfolios, audits, and internal control audits or opinion audits, as well as NCUA exams and state exams for state-chartered credit unions
- Review board minutes and interviews with staff and board members to discover any areas of concern
- Check and validate employee and volunteer personnel files to ensure there are no current or past dishonesty, fraud, or Bondability issues. Remember, a loss discovered by the previous organization can impact your insurance coverage going forward. Review Unreported Prior Acts to learn more about minimizing the impact to potential claims and/or Bondability issues.

MEMBER COMMUNICATION. It can be the difference between a successful merger and a chaotic one. Follow federal and state timelines regarding merger communication to all, including member groups, regulators, and the media. Share the announcement to both membership bases at the same time and maintain consistent, frequent updates on merger progress and important timelines. Using a FAQ document is a common practice, as well as preparing call centers for increased activity.

EXPECT THE UNEXPECTED. Strategic M&A decisions should be carefully considered to ensure that hidden costs and risks are properly identified and analyzed. Be aware of redundant systems, assets, contracts, applications and processes. Be certain your organization is proactively addressing exposures before the deal is signed.

James Bullard
Senior Risk Consultant
CUNA Mutual Group

"Mergers and acquisitions can drive measurable benefits for credit unions and their members. However, they are a time-consuming and emotional process that can come with unanticipated complications, challenges, and mistakes if proper oversight is not in place throughout the entire process."

Digital Lending

The digital imperative.

Consumer behavior is telling credit unions that they want fast and simple solutions that link with their connected lives.

Digital Lending's end-to-end journey necessitates no authentication breaks

We live in an increasingly digital world. Retailers prefer to email your receipt. Mortgage closing attorneys provide borrower copies of closing documents in electronic format. Ultimately, digitization is about adapting to compete in an increasingly digital world.

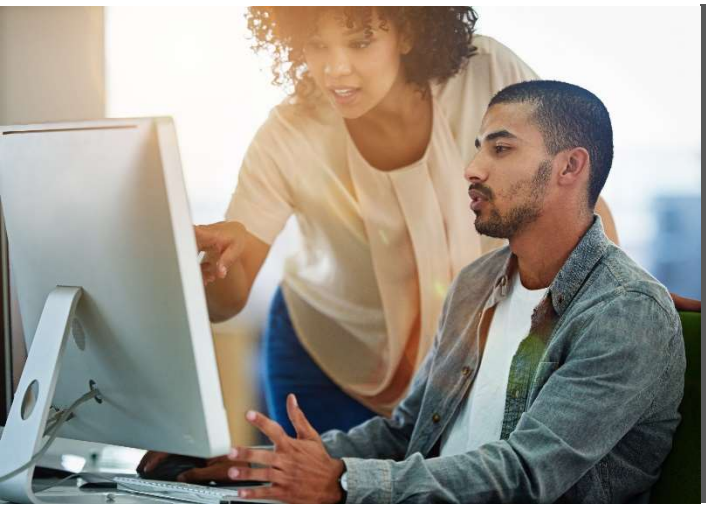
The lending function for credit unions is no different. Credit unions are as diverse as their members and are faced with finding ways to maximize success by embracing the digital lending landscape. Competition is forcing this change. The traditional consumer lending process has just about become obsolete in terms of efficiency and access to members. And, a digital lending program is more than providing a mobile app.

Digital technology is transforming the process by providing credit union members with simplicity, efficiency, and transparency.

- **Simplicity:** Implies convenience and flexibility. Members want to be able to apply on their schedule, wherever they are, and using the device of their choice.
- **Efficiency:** The process should be quick, seamless, and provide consistency across channels. The process should include the ability to upload supporting documents without leaving the application as well as the ability to receive a decision in minutes and sign documents electronically.
- **Transparency:** Removing human interaction from the process creates the need for increased transparency. This includes providing information about the steps and timing of the process and disclosure of the loan details.

"Digital lenders in particular are ripe for target by fraudsters since they emphasize speed and application efficiency over fraud prevention"

Source: LexisNexis® Risk Solutions,
2019 Small and Mid-Sized Business Lending Fraud Survey



The Digital Challenge

- Balance virtual convenience with transaction security
- Enforce security with little impact on experience
- Require member authentication and validation at each layer of the digital channel and transaction

Reducing Friction & Improving Consistency

Success in the digital landscape depends on the ability to eliminate friction and provide consistency across all channels. Regardless of operational structure, the member expects a seamless experience.

This seamless, digital experience includes:

- Full integration means the ability to switch methods of engagement, i.e. from a mobile device to a branch or call center.
- The ability to save an application, at any point in the process, and resume later, potentially on a different channel. This is necessary to reduce abandoned applications.
- Efficiency delivered through a robust decision engine which blends the same look and feel with the ability to return a prompt decision. The industry standard is approaching 30-seconds from submission to decision.
- To be truly digital, the availability of eSignatures is a given. Having eSignature functionality, and employing all available authentication methods, is key to providing an excellent digital experience.

What's the risk?

The most risky step in the process may be the functionality to verify information provided in the application, such as identity, income and employment. You're encouraged not to cut costs by skipping this step. Any break in the **member authentication process** opens the door to loan fraud.

Lenders committing to an elevated customer experience is a good thing, but it creates the perfect environment for fraud. Focusing on streamlining the loan process can make it easier for fraudsters to cheat the system.

Loan staff who process loan applications should be trained on **how to spot fraudulent applications**. They should carefully scrutinize credit reports and other support documents to identify red flags.

The digital channels are prime opportunities for fraudsters given the anonymous environment and ability to send multiple applications at the same time to different lenders (loan stacking).

Conclusion

The expectations of the digital borrower have shifted. While the interest rate and closing costs on loans are still primary considerations; the speed, simplicity, transparency and member service aspect is growing in importance.

Outsmarting the fraudsters starts with having the right toolset, oversight, and a multi-layered fraud strategy that supports a 360-degree view into the lending business.

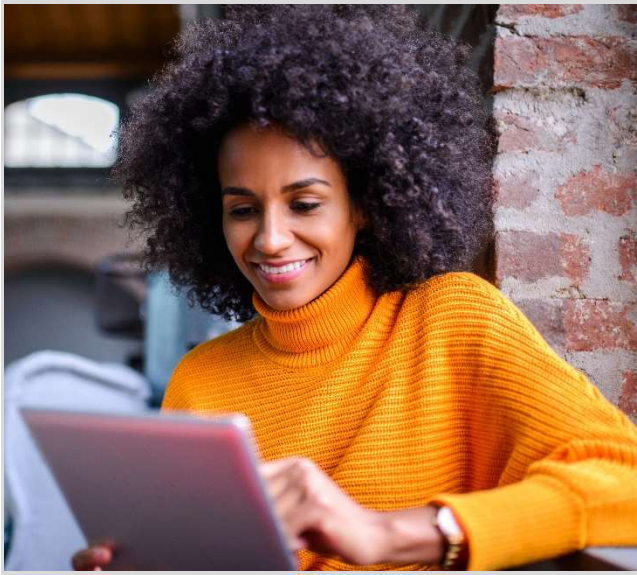
TRENDING

The pace at which consumers adopt technology has quickened significantly.

Time to reach 50 million users

19 days	Pokémon GO
6 months	Instagram
3.5 years	Facebook
13 years	Television
35 years	Radio
75 years	Telephone

Source: Visual Capitalist



Borrowing preferences of consumers are shifting.

TODAY

About 30% of loans are originated or funded online

2020

Over 80% of loans will be originated online according to industry forecasts

Cannabis Impact

The cannabis conundrum.
The legalization of cannabis across the country presents uncharted territory for many credit unions.

A business decision complete with uncertain risks and a hazy future

Risks & Drugs in the Workplace

- Medical use and job safety: In situations where cannabis is used to aid a disability, reasonable accommodations must be made, but not at the expense of safety. Health and safety should take priority.
- Debate and questions center around if Workers Compensation claims can be made if an employee was using medical marijuana when injured or if the credit union is required to pay for it as a treatment after a workplace injury.
- Credit unions need to evaluate drug and alcohol policies to ensure compliance with not only federal and changing state laws, but also with an eye for the increasing shift social perceptions that may influence their current and potential workforce.
- While making it clear that on-the-job consumption or being under the influence of cannabis, marijuana and/or any other substances remains against credit union policy, any current or developing testing protocols may also need to be reevaluated.

For additional risk insights and mitigation tips:

- Serving Marijuana-Related Businesses Risk Overview
- Employer Risks, Rights & Obligations eBook
- Lending to Marijuana-Related Businesses

Providing services to marijuana-related businesses requires a tremendous amount of work and expertise. Credit unions contemplating offering these services should proceed cautiously, especially in light of the heightened due diligence and changing regulatory environment.

Serving Cannabis-related Businesses

Credit unions that are considering offering account services to marijuana-related businesses (MRBs) face a dilemma. While several states plus the District of Columbia have legalized marijuana in one form or another, it's still illegal at the federal level under the Controlled Substances Act. Therefore, handling the proceeds of a marijuana transaction could be viewed as money laundering. That's why so few financial institutions open accounts for MRBs.

The Department of Justice (DOJ) issued guidance to federal prosecutors in 2013 indicating that while marijuana remained illegal under federal law, federal law enforcement officials would not interfere in states where marijuana is legalized as long as they enforce certain priorities (enforcement priorities). In response to the DOJ's guidance, the Financial Crimes Enforcement Network (FinCEN) issued guidance to financial institutions in 2014 (BSA Expectations Regarding Marijuana-Related Businesses) wishing to provide depository services to MRBs and remain in compliance with BSA laws.

FinCEN's Guidance

It's imperative for credit unions contemplating offering depository services to MRBs to proceed cautiously. Providing depository services to MRBs is not a turnkey operation. Rather, it takes a tremendous amount of time and effort to comply with FinCEN's guidance for banking MRBs.

The decision to provide depository services to MRBs ultimately resides with the credit union's board of directors. This decision should only be made after senior management has conducted a thorough risk assessment considering FinCEN's guidance to identify the risks and making a realistic determination of whether the credit union can effectively manage those risks.

Evaluate your credit union's ability to comply with FinCEN's guidance:

- Do you have a strong BSA/AML program?
  - How did you fare in your last BSA/AML audit?
  - Were weaknesses identified adequately resolved?
- Are existing BSA/AML staff certified?
- Will you need more staff with strong BSA/AML backgrounds?
- Do you have a thorough understanding of your state's licensing requirements?
- Can you effectively comply with the expected level of enhanced due diligence in the onboarding process?
- Can you effectively perform ongoing monitoring of MRB relationships including on-site visits?
- Can you effectively monitor for suspicious transactions including red flags described in FinCEN's guidance that implicate an enforcement priority?

Conclusion

Providing depository account services to marijuana-related businesses requires a tremendous amount of work and expertise. The decision to open accounts for marijuana-related businesses resides with your executive leadership and board of directors and should be made only after an evaluation of your credit union's objectives, an evaluation of the various risks, and an honest determination of whether the credit union can effectively manage those risks.

TRENDING

SAFE Banking Act could facilitate financial services for cannabis

Relief may be on the horizon for financial institutions wishing to bank MRBs in the form of the Secure and Fair Enforcement Banking Act of 2019 (SAFE Banking Act). The SAFE Banking Act offers a safe harbor to financial institutions, insurance companies and other parties seeking to provide services to MRBs in states where marijuana is legal.

Additional Risk Considerations

- Banking MRBs will potentially result in a substantial increase in share deposits. Credit unions should have a plan for how they will use the increased share deposits. To manage this risk, establish a limit on MRB shares as a percentage of net worth.
- Ensure you can effectively manage MRB accounts. A best practice is to establish a limit on the number of MRB accounts to accept into the program, such as limits by type of license (producer, retailer, etc.).
- Robbery/burglary exposures will increase if MRBs make cash deposits at a branch. Evaluate branch security including safes, vaults, alarm systems & armored car service.
- Credit unions offering wire transfer service to marijuana-related businesses should adopt a written wire transfer agreement due to the potential size of their wire transfer requests.
- Be sure to qualify MRBs for checking, debit cards, remote deposit capture, and ACH origination like you do for other types of businesses.
- Credit unions should exercise extreme caution with lending to marijuana-related businesses. One potential risk is the seizure of a marijuana-related business' assets which are being used as collateral on loans.
- Reputation risk with your members and/or community stakeholders who may object to the type of business is also a significant consideration.

Member Authentication

Assault on Authentication.

Account takeover losses more than tripled in the last year to $5.1 billion.

Source: Javelin Strategy & Research 2018 Identity Fraud Study

Knock…knock. Who's there?

Losses from account takeovers through online banking are increasing at an alarming rate. The online channel provides a cloak of anonymity for fraudsters, making it critical for staff to be alert and cautious when opening accounts and processing loan applications. There are two primary ways fraudsters perpetrate account takeovers through online banking:

- Enroll member accounts for online banking through credit union websites by exploiting weak authentication methods; and
- Compromise login credentials including out-of-band authentication leveraging one-time-passcodes (OTPs).

Online Banking Enrollment

The starting point for mitigating the risk of account takeovers through online banking is to properly authenticate members enrolling for online banking through credit union websites. Members enrolling for online banking through credit union websites are frequently authenticated by asking for personal information (e.g., account number, address, phone number, date of birth, email address, etc.) which is reviewed for accuracy before they are granted access to online banking. This method of authenticating members is weak and has resulted in fraudsters enrolling member accounts for online banking.

Consider deploying an out-of-band authentication method for this purpose. This typically involves generating a one-time-passcode (OTP) which members must enter to complete the enrollment process. Members are given a choice in how they want the OTP delivered, such as by automated phone call, email or SMS text message. Avoid sending OTPs via email due to the risk of member email accounts being hacked. In fact, several losses involving account takeovers have occurred when fraudsters hack member email accounts to intercept OTPs. Sending OTPs in SMS text messages is also risky – but not as risky as email.

Data breaches have fueled the problem since they often lead to identity theft. The uptick in Social Security number compromises, in addition to other personally identifiable information (PII) – names, addresses, and birthdates - from these breaches compounds the problem.

Out-of-Band Authentication

Multifactor authentication by itself is not sufficient to mitigate the risk of account takeovers through online banking. That's why credit unions are deploying out-of-band authentication - a layered security tool - leveraging the use of OTPs. Out-of-band authentication should be used in several situations including:

- When a member attempts to login to their account using a device not recognized by the host system;
- When a member changes their contact information and/or password through online banking's member profile feature;
- When a member initiates a transaction exceeding a monetary threshold; and
- When a member uses the "forgot password" feature

An OTP is generated when out-of-band authentication kicks in and, as mentioned above, the member is given a choice in how they want it delivered – by automated phone call, email, or SMS text message. Upon receipt, the member is required to enter the OTP to complete the transaction.

Fraudsters have adapted to this out-of-band authentication method and deployed tactics to intercept OTPs transmitted to members:

- Hacking member email accounts to intercept OTPs;
- Infecting member mobile devices with mobile banking Trojans (a form of mobile malware) or SMS malware to redirect text messages to the fraudsters;
- Porting member mobile devices to a different carrier without the member's knowledge; and
- Social engineering a member's mobile phone carrier representative into issuing a replacement SIM card

To effectively mitigate the risk of fraudsters intercepting OTPs, credit unions should deploy a secure app-based method of pushing OTPs to the dedicated app that resides on members' mobile devices.

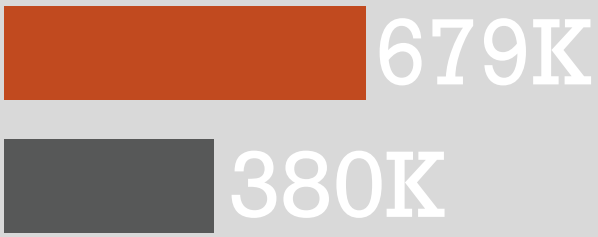
Conclusion

Member authentication tools and tactics have evolved over time. But, fraudsters continue to impersonate members to carry out fraudulent transactions.

The online channel has quickly become a valuable tool for credit unions in providing member convenience – like account opening, loan applications, and other banking transactions. However, this also provides fraudsters with another channel and one with more obscurity challenging credit unions in properly authenticating and verifying members and potential members.

Account Takeover

Mobile phone account takeovers are on the rise



14.4 million consumers fell victim to fraud

"High-impact fraud types like account takeover and new account fraud remain alarmingly common, demonstrating that fraudsters continue to find and compromise new targets."

Source: Javelin Strategy & Research
2019 Identity Fraud Study

Talent Management

A strategy for your credit union's future.

The ability to hire and retain skilled employees and manage the risks associated with developing critical and top talent plays a key role in sustainable business success.

Transforming your workplace

The employer / employee relationship is evolving rapidly and with both sides held to a higher standard. Employees expect personalized, accountable workplaces from their employers. In return, employers expect employees who are not only technically proficient, but who can think creatively, collaborate, and adapt along with the constant pace of change.

Three Trends Demonstrate Talent Management Dynamics

89%
suggest bad hires typically lack soft skills

Soft Skills

While soft skills have always been important, they are even more in demand today as the rise of task automation points to the potential irrelevancy of technical "hard skills." Technical competency may have been enough to predict a successful employee in the past; however, organizations now point to hiring for skills such as creativity, persuasion, collaboration, and time management as a priority.

Credit unions need to identify which skills they will prioritize, how they plan to assess for those skills (online or via interview questions), while being mindful of individual or organizational bias that may creep into the assessment process.

79%
increase in LinkedIn job postings mention work flexibility

Work Flexibility

Empowering employees to work when and where they want is quickly becoming a standard of workforce management. Credit unions that can adapt to meet these demands are going to be in a uniquely better position to attract and retain top talent.

Issues like team bonding, collaboration, and oversight may be initial challenges; however, adopting technological solutions such as instant messaging and video conferencing platforms may address these challenges. These tools allow employees to work in different locations and time zones while creating the sense of being in the same location as their peers.

52%
pay is very important to the future of recruiting and HR

Transparency & Accountability

Key legal and workplace morale issues - such as harassment and pay inequality - have plagued many a workplace. The credit union industry is not immune. Recent trends have shown applicants and employees alike are demanding that employers do better in addressing these issues.

While harassment and pay equity have historically been confidential topics in the workplace, the benefits of transparency may outweigh these fears. Being upfront about expectations with candidates related to standards of behavior and compensation address the potential for confusion and foster a more trusting relationship with employees.

Source: 2019 Global Talent Trends, LinkedIn Talent Solutions

Business Resiliency

Weathering the storm.

Ten U.S. weather events alone – three floods, five severe storms, and two tropical cyclones - caused losses exceeding $1 billion each through September 2019.

Be prepared to survive and thrive when the climate strikes

C-Suite

Key Climate Questions

Chief Sustainability Officer

- Do we have an initial list of top climate risks facing the credit union?
- What data – impact and frequency – do we have on these risks?
- Are we regularly providing this data and insight to risk management and finance?

Chief Risk Officer

- How are climate risks captured in the risk identification process?
- Ave we mapped these risks and their impact to the credit union's performance?
- How are regularly updating these risks?

Chief Financial Officer

- Do we understand the financial impact of climate risks on the credit union?
- How do climate-related risks serve as an input to financial planning?
- How are we reporting the risk impact to the Board and executive leadership?

Chief Investment Officer

- Have we considered we considered climate-related risks and opportunities for our investment strategy under different climate scenarios?
- Are these risks included in investment decisions?

Even when extreme weather doesn't produce damage, weather-related power outages such as those experienced in California in 2019 can cost billions in financial loss. In fact, the Federal Emergency Management Agency (FEMA) estimates that 40 percent of businesses do not reopen after a disaster, and another 25 percent fail within one year.

Business resilience refers to a state of continued, uninterrupted operation of business functions. It focuses on the resiliency of people, property, processes, platforms and providers. A credit union that is resilient to climate events is an organization that has built the capacity to adapt and succeed in the face of the direct and indirect impacts of a disaster.

The credit union's objectives of business continuity should be to:

- Keep people and property safe
- Protect vital assets owned by the credit union and those assets belonging to others responsible
- Protect intellectual assets and contracts that effect credit union supply chains
- Preserve the ability to meet all stakeholder expectations
- Maintain or gain competitive advantage due to a swift and effective response

Assess vulnerabilities of your operations & facilities

Extreme weather events can have devastating effects on property and infrastructure with lasting impacts. These events can affect multiple supply chains and can significantly erode profitability lines.

Leverage enterprise risk management (ERM) and risk assessment processes to increase awareness of climate risks. Incorporate a framework into your risk identification processes to map how climate affects all assets, product lines, and the member experience. Additionally, ensure staff has the proper training so they can respond efficiently and effectively when their role is needed during an unfortunate climate event.

Governing Cyber Risk

Prevention is better than cure.

Cybersecurity spending on technology is expected to increase, in addition to more focus on planning, employee training, cybersecurity staffing and third-party services

Source: Hiscox Cyber Readiness Report 2019

Cybersecurity: one of the most dynamic risks for the C-suite to manage

Cybersecurity governance is dynamic risk area where credit unions need to adapt and adjust their priorities accordingly. A few of the fundamental components that should be clearly defined: Cybersecurity Strategy & Goals, Senior Leadership Oversight, and Cybersecurity Legislation.

CYBERSECURITY STRATEGY & GOALS

Establishing a quality cybersecurity governance program begins with risk management policies, a guiding strategy, and stated goals. The credit union's risk appetite should drive strategy and goals for the credit union's desired governance posture. Strategy should be articulated by senior leadership at a high-level an establishes a roadmap to an enterprise level policy. A few key components to this strategy should be:

- Determining a risk appetite
- Identifying how cybersecurity risk relates to all critical business operations
- Establishing key performance indicators (KPIs) as well as key risk indicators (KRI)
- Identifying cybersecurity needs, objectives, and desired resources
- Call for an environment of continuous monitoring

SENIOR LEADERSHIP OVERSIGHT

Cybersecurity governance is an operational enterprise wide concern. The focus and direction must come from the top to ensure that the process is successfully adopted. Without a "tone from the top" approach, the credit union's efforts will most likely fail.

Senior leadership should be responsible for:

- Ensuring that established governance policy and objectives are compatible with the strategic direction
- Confirming governance policies and objectives are communicated to all relevant parties
- Require governance protocols be integrated into all credit unions processes and business lines
- Reinforce a commitment to continual improvement

Active C-suite engagement will help executives gain a clearer perspective on how effective their data security plans are and what needs to be done to make improvements. C-suite leaders need to actively engage with and guide that strategy so it becomes a part of your credit union's fabric.

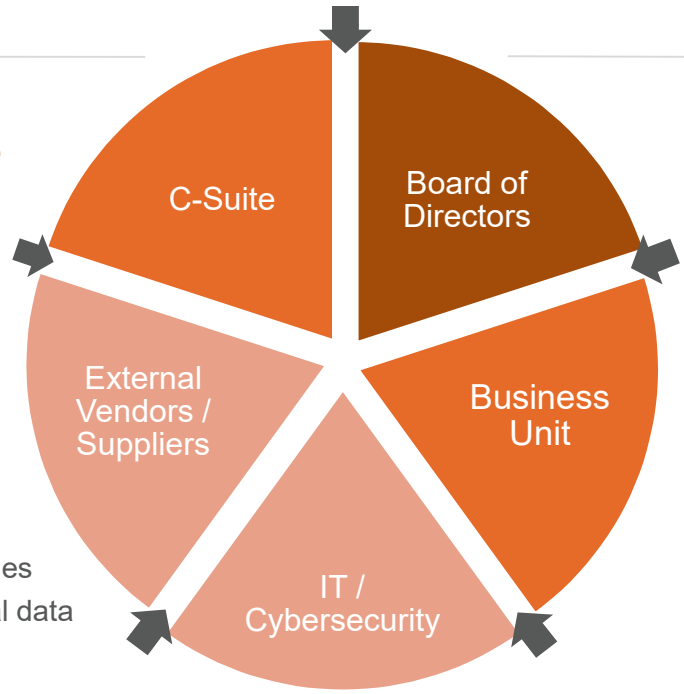
CYBERSECURITY LEGISLATION

State legislatures continue to advance proposals to address cyber threats by making protective cybersecurity measures a priority. In 2019, 43 states and Puerto Rico introduced or considered close to 300 bills dealing with cybersecurity. These cybersecurity-related legislations deal with issues such as required training programs, the use of advanced technology for security purposes, enhanced breach notifications, and addressing the security of connected devices.

This increased legislation will create challenges for credit unions as they may be responsible for complying with regulations from multiple jurisdictions and multiple regulators. Once formal regulations are established credit unions will need to figure out how to achieve an efficient and effective control framework for compliance.

On the upside, a comparison of the detailed requirements generally reveals many commonalities among these multiple regulations that may in some cases simplify the task of cyber governance. With the right subject matter experts and approach, compliance is an achievable goal.

The most important factor in any cybersecurity program is trust, according to McKinsey Digital. Cybersecurity trust gaps can exist on many levels across the organization ecosystem.



The board must have trust in the C-suite and its ability to handle cybersecurity without dramatically affecting the credit union's value and brand. The C-suite needs to trust the chief information security officer's claims that the budget spent on improving the IT infrastructure is worth it. The credit union needs to trust that vendors can properly protect shared corporate and member data or ensure service stability if breaches occur. And, of course, members need to trust that their personal data is being carefully safeguarded behind corporate walls.

Cybersecurity needs to run horizontally through your entire credit union. It is not just an IT problem. With so much at stake, cybersecurity must be a top-tier risk that receives the full attention at your credit union. Engage the C-suite to create a culture of engagement and accountability to ensure that your cybersecurity roadmap connects with your credit union's goals and objectives.

Next Gen Defenses

Use of risk data remains a stumbling block.
The C-suite wants to see data and analytics used with decisions on specific risks and to inform the overall business strategy.

Using Data Analytics to Support Strategy & Control Losses

AI and Machine Learning Benefits

- Account Opening and Loan Evaluation: Validate the authenticity of applicant information to improve accuracy and efficiency.
- Payment Authorization: Evaluate requests and authorize payments in real-time
- Improved Fraud Prevention: Reduce manual review of queues through fast iterating machine models. Reduce false positives with behavior analysis.
- More Accurate Product Recommendations: Augment human decision-making with increased precision
- Personalized Communications and Advice: Applications like online virtual advisors can offer members real time accurate account solutions and financial advice
- Improved Productivity and Efficiency

Often used interchangeably, Machine Learning and Artificial Intelligence (AI) are two technologies that are likely to continue influencing the way credit unions view and service their members. After several years of anticipation, these disruptors are finally being more widely adopted by loss and fraud prevention specialist seeking to improve their security posture. Business strategists and other senior leaders are also finding ways to leverage these tools to improve processes, eliminate inefficiencies and offer customized solutions to their members.

ARTIFICIAL INTELLIGENCE IN ACTION

Artificial Intelligence refers to the vast umbrella of systems or applications that leverage data and information to perform tasks previously completed by humans. One of the earliest uses of artificial intelligence in financial institutions was to improve fraud detection. Real-time monitoring of account activity allowed for the identification of patterns and led to easier recognition of irregularities within those patterns to be flagged for further review.

As AI technology evolved, we were introduced to possibilities like self-driving cars and virtual assistants. More applicable uses of AI for credit unions, today, include systems designed to allow for more accurate product recommendations, stronger underwriting, and personalized member communications.

A MORE DETAILED VIEW OF MACHINE LEARNING

Conceptually, machine learning is the field of study that gives computers the ability to learn without being explicitly programmed. In application, it seeks to extract meaningful information from data; to solve problems that otherwise cannot be solved by numerical means alone. The discipline includes a growing number of subsets all of which improve over time as more data is processed, and more positive results achieved.

Machine learning is the backbone for a wide range of critical applications, such as data mining, natural language processing, image recognition, and many fraud prevention solutions. Because fraud mimics good consumer behaviors, our best members are often penalized by over-intrusive mitigation strategies. Machine Learning directly addresses labor intensive activities like transaction and false positives reviews to help reduce resource consumption and improve the effectiveness of fraud prevention.

Additional Considerations:

- Steep learning curve and talent shortage can make these technologies difficult to implement
- Siloed data sets can pollute information
- Expensive to purchase and integrate into business models
- Chance of poor output: Although Artificial Intelligence can learn and improve, it still can't rationalize; therefore, is subject to irrational decisions unless there is human intervention. AI might never be able to take individual circumstances and judgment calls into account when making decisions.

Conclusion

Most credit unions are only in the early stages of adopting AI technologies as they pursue a stronger understanding of member behaviors and execute fraud detection strategies. Given the sophistication and speed of organized fraud rings credit unions will certainly benefit from continued exploration of these solutions. Further, as credit unions continue to embrace technology in efforts to offer more customized solutions to their members the benefits of leveraging AI and Machine Learning are undeniable.

A disconnect between how C-suite and risk executives view analyzing data

#2 gap:

C-suite said analyzing risk data is the second largest gap in risk management's overall performance

#10 gap:

Risk executives said it was far down the list of problem areas

Source: 2019 Excellence in Risk Management Report, Marsh & RIMS

Employee / Workplace Safety

Safety plans and employee actions.

A focus on workplace safety demonstrates your commitment to keeping your employees safe, secure, and even helping make them more productive and happier at work.

Instill a culture of employee safety first

Workplace safety starts with a strong safety culture, the collection of value and beliefs that employees share in relation to risks in the workplace. Effective leadership and employee engagement is critical. And, with changes in today's environment, credit union employees must also exercise caution.

Unfortunately, workplace injuries cost businesses billions of dollars each year. You're either prepared or unprepared and that's something that needs to be prioritized. These two risks are of significant concern.

Responding to Active Assailant Events

79%

feel a little bit or not prepared for an active shooter incident.

Source: Everbridge, Active Shooter Preparedness Research Report

It has become more common in our everyday lives. Tragic active shooter / assailant events are unpredictable and evolve quickly. Individuals must be prepared both mentally and physically.

While it is somewhat like trying to teach instinct, employees should have a clear understanding of:

- Your credit union's Emergency Action Plan
- The everyday surroundings and know they have the authority to take immediate action to protect themselves
- Potential scenarios and how to respond
- Expectations from first responders

Managing Workplace Safety

51.8%

of slip, trip & fall claims are within the 50-59 and 60-69 ages.

Source: 2017-19 CU claims data The Hartford

Periodic inspections of potential hazards are often limited to unsafe physical conditions; however, employee safety risks can also be due to safety alertness and unsafe work methods and practices.

- More than 1,000 Workers Compensation claims totaling **$3.9 million** have been incurred by credit unions from 2017 to August 2019, according The Hartford
- Slip, trip & fall, in addition to ergonomic claims, have seen an increase in losses based on age
- Employees involved in a loss miss an average of 38 work days as reported by CUNA Mutual Group partner, M3 Insurance

"Most importantly, credit unions need to develop a plan for a safe environment in each type of location. We all know that no two branches are the same."

Carlos Molina
Senior Risk Consultant
CUNA Mutual Group

Conclusion

With careful assessment, planning and implementing sound policies and procedures, you can proactively demonstrate your commitment to your employees and proactively minimize preventable workplace injuries. Your focus should give every employee the information they need on how to handle certain situations, whether it's a fire in the breakroom, a spill in the hallway, or an unfortunate, traumatic event.

It's a Wrap.

When risk management is effective, typically nothing bad happens. 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.

Establish a sound strategy and risk relationship.

Handling emerging risks is not an easy task. Along with a strong leadership team, it requires organizational agreement on your strategic direction, risk philosophy and appetite. Everyone needs to understand the credit union's capacity to take risk and your tolerance for potential loss.

Your strategy and risk relationship should help you embrace uncertainty allowing you to get even more strategic with your risk decisions. However, know that the risk management discussion should not be about yes or no; rather it is the opportunity to take a broad look at all risk factors with, at minimum, these components in mind:

- **Objectives:** Where are we going?
- **Initiatives:** How do we get there?
- **Risks:** What could go right / wrong?

Keep your head on a swivel as emerging risks are relentless.

Internal and external risk events affecting the achievement of your objectives come at you from all directions and through many different credit union functions - some of these risks are repeat offenders and others are just being introduced for the first time. Credit unions that stay current on risk trends and integrate risk management into their day-to-day strategies, business plans, and operations are typically more likely to minimize their losses related to emerging risks.

Risk & Compliance Solutions • 800.637.2676 • riskconsultant@cunamutual.com