2021 eBook Series updated 07/2021

RETHINKING PROTECTION

emerging risk outlook

Risk & Compliance Solutions
800.637.2676
RiskConsultant@cunamutual.com

CUNA MUTUAL GROUP

CUNA MUTUAL GROUP

emerging risks
in an era of uncertainty

Ransomware

Ransomware has grown in frequency and severity and extortion demands have risen significantly. A ransomware incident is one of the most disruptive and costly attacks your organization can suffer.

Authentication

The online channel and changed business practices provide a cloak of anonymity for fraudsters, making it critical for staff to be alert and cautious when opening accounts and processing loan applications.

Operational Considerations

New work environments and external forces drive risk related to Employee Safety & Wellness • Remote Working Capabilities • Physical Asset Management • ATMs

Fraud & Scams

Fraudsters have jumped on the opportunity to exploit weak security measures (P2P, kiting, fraudulent instruction) as employees and members adjust to a new environment.

Internal Controls

Adjusting operations and business practices can result in more lax internal controls. In fact, Employee & Director Dishonesty and Faithful Performance account for 47% of Bond claim dollars paid over the last 5 years (Internal Claims Data, CUNA Mutual Group).

Employment Practices

Risks related to different remote management styles, cultural issues, rethinking roles and even staff reductions can drive potential risk and litigation.

Business Resiliency

The perfect storm of challenges in 2020 highlighted the importance of deliberate business resiliency planning. Many found not all plans were fully sufficient.

.

Default Management

Collections is a balancing act - between being empathetic while members are under financial stress and needing to collect on loan debt. It is critical to rethink your loan and collection strategies.

Digital Transformation

The pandemic influences on member preferences are far-reaching. Strategic decisions to move forward with a digital transformation should carefully consider risks too.

Mergers & Acquisitions

M&A can drive measurable benefits. However, they can come with unanticipated complications, challenges, and mistakes if proper oversight is not in place.

Compliance & Litigation

As regulations and litigation across the financial services industry evolve, credit unions must work to understand and revamp compliance initiatives.

These cyber attacks have no boundaries and are truly a global issue. Ransomware has grown in frequency and severity and extortion demands have risen significantly. A ransomware incident is one of the most disruptive and costly attacks your organization can suffer.

Average Ransom Payment in Q1 2021 [1]

43% leap from Q4 2020 average

Percent of increase in claims from 2018 to 2019 [2]

Payments have increased 228% during the same timeframe

Average days of downtime [1]

Sources:

[1]Coveware Quarterly Ransomware Report – Q1 2021
[2]Beazley internal claims data - 2020

Six- and Seven-figure Demands

Ransomware developers and affiliates have been telling victims that they must pay the ransom or stolen data and internal company secrets would be publicly released. Unfortunately, six and seven-figure demands have become routine among ransomware attacks.

Data Reveal

The fact that ransomware attackers can steal as well as encrypt data isn't a new phenomenon but the possibility that sensitive data might be revealed to the world is potentially more damaging than any short-term disruption caused by the malware.

Data could include member financial records, employee personal information, termination letters, salaries, and much more.

Most Identified Infection Points

- Weak remote desktop protocols (RDP)
- Phishing / Spear Phishing emails
- Corrupt attachments
- Unpatched system vulnerabilities and untimely anti-virus updates
- Extensive reuse of passwords
- Lack of multi-factor authentication

Dwell Time

More effort is being placed towards remaining undetected on a breached network - commonly referred to as dwell time or the time that exists between the first execution of malware and its discovery inside the network. The average dwell time is 43 days for ransomware according to Infocyte.

Ransomware as a Service

Ransomware code on a reseller distribution network is a very lucrative business for cybercriminals. The availability of free, do it yourself ransomware-as-a-service (RaaS) kits, and cheap attack ingredients pushed the barrier to entry extremely low. Deep technical expertise is no longer needed to participate in the cyber crime economy.

1. Initial compromise of your environment

Remote Access Security

- Microsoft RDP and Remote Desktop Gateway (RDG) can be used to provide remote access to computers and networks.
- RDP/RDG attacks are an attractive and common way for hackers to access systems and steal valuable information from devices and networks.

Phishing / Spear Phishing

- Fraudster or criminal group targets your organization with a phishing campaign.
- Spear phishing targets a select group with something in common – e.g., work or bank at the same organization.
- Malware is successfully delivered to one of your unsuspecting users via a malicious attachment or web link in an email.

2. Malware is installed

- The user opens the attachment and malware is unknowingly installed on the user's PC to gain a foothold in your environment.
- The hackers undetectably explore your network looking for vulnerable systems and sensitive data - including other users' PCs and servers supporting critical applications and file stores.

3. Ransomware is deployed

- With access achieved, ransomware is spread across your network encrypting indiscriminately.
- The attackers have now encrypted and disrupted a material portion of your business. Some parts of your business are completely disrupted while other parts are partially disrupted.

4. Extortion

- The attackers demand a ransom – up to millions of dollars - for the decryption key.
- The attack can also become public knowledge which causes reputational damage. The regulator also wants to understand if there has been a mishandling of customer sensitive data.

Related Resources

- Cybersecurity Threat Outlook eBook
- Ransomware Risk Overview
- Ransomware Prevention & Response Checklist
- Mobile Device Risks & Security Risk Overview
- Business Email Compromise Risk Overview
- An Employee's Guide to Phishing Emails

PROACTIVE PREVENTION

- **Patch and Update**
  Keep all systems including hardware, mobile devices, operating systems, software, cloud locations, and content management systems (CMS), patched and up-to-date.
- **Multi-Factor Authentication**
  Activate two-factor / multi-factor authentication (2FA/MFA) on all systems — including managed service provider software platforms, administrator systems, and end-user systems wherever possible.
- **Data Backup**
  Backup data regularly and routinely test backups for data integrity.
- **Apply the principles of least privilege and network segmentation**
  The end user should be given only the privileges necessary to complete tasks related to their role in the credit union. If an employee does not need an access right, the employee should not have that access right.
- **Engage Employees**
  Provide frequent social engineering and phishing training to o employees so they can become an effective first line-of-defense.
- **Monitor Third-Parties**
  Vet and monitor third parties that have remote access to the credit union network and connections to third parties. Ensure they are diligent with cybersecurity best practices.
- **FinCEN's Red Flag Indicators**
  Familiarize yourselves with FinCEN's Advisory (October 1, 2020) and the list of 10 financial red flag indicators to assist in detecting, preventing, and reporting suspicious transactions associated with ransomware attacks.

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.

$16.9 Billion

Estimated identity fraud losses [1]

1-in-20

American consumers victimized by identity fraud-related financial losses [1]

69%

Worried about the theft of customer data through mobile security threats [2]

Sources:

[1]Javelin 2020 Identity Fraud Study Genesis of the Identity Fraud Crisis

[2] Verizon Mobile Security Index 2020

Two Primary Ways Fraudsters Perpetrate Takeovers

- 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).

Identity Verification

Members enrolling for online banking through credit union websites are frequently authenticated by asking for personal information (e.g., account number, address, phone # , date of birth, email address) which is reviewed for accuracy before they are granted access to online banking. This method of authentication is weak and has resulted in fraudsters enrolling member accounts for online banking.

Strong Out-of-Wallet Questions

- What year did you open your account?
- Who is the payable on death beneficiary on your account?
- What is the last loan you paid off with the credit union, approximate date and collateral used?

Out-of-Band Authentication

Deploying an out-of-band authentication method for online banking enrollment through credit union websites is a growing practice. The same should be used for your employees accessing your systems in order to mitigate against unauthorized access to credit union data.

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.

Out-of-band authentication should be used in several situations:

- 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

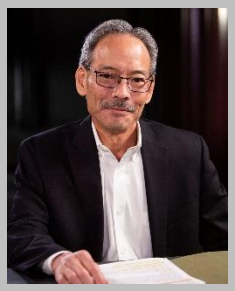
Fraudsters' Tactics to Intercept OTPs

Fraudsters have adapted to out-of-band authentication method and deploy 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.

Transmitting OTPs via email is best to be avoided due to email's inherent risks (i.e., email accounts can be hacked). In addition, transmitting OTPs via SMS text message can be defeated if a member's mobile phone is fraudulently ported to a new carrier. Credit unions should assess these risks when considering this out-of-band authentication method.

Although out-of-band authentication is considered an effective layered security control for online banking, fraudsters are obtaining the OTPs by targeting the weakest link - your members - through sophisticated scams.



Ken Otsuka
Senior Risk Consultant
CUNA Mutual Group

Ken shares more insights in this video!

Two-Factor Authentication Risk Overview

Other Common Identity Theft-related Fraud

- **New Account Fraud**
  New account fraud losses are increasing through the online channel. Fraudsters who open accounts at credit unions typically use stolen identities. In addition, these fraudsters make fraudulent deposits of checks or ACH debits and withdraw the funds before the items are returned unpaid to the credit union.
- **Loan Fraud**
  Losses stemming from identity theft-related loan fraud tend to be more severe in dollar amount than the losses associated with new account fraud. Once a fraudster opens an account, usually through the online channel, they immediately apply for loans, including unsecured loans, credit cards, and vehicle loans. These losses are increasing as more credit unions accept loan applications through the online channel.
- **Call Center Fraud**
  Fraudsters frequently target the call center and often request changes to members' contact information (e.g., phone number, email address, etc.) which typically leads to other forms of fraud, such as requesting wire transfers through the call center.

Multifactor Authentication Bypass

Multifactor Authentication bypass should be a significant concern according to Sherri Davidoff of LMG Security. The primary vulnerability here begins with passwords.

Unfortunately, researchers uncovered over **15 billion stolen passwords traded on the dark web**, which enable cybercriminals to easily purchase credentials for online banking accounts or remote login interfaces.

These criminals then use these passwords and attempt to login into other web sites. Since approximately **65% of people re-use the same password for multiple accounts**, these credential stuffing attacks are effective and an easy way for even low-tech criminals to break into accounts.

Credit unions have a responsibility to protect employees, members, and visitors by taking measures to detect potential incidents, manage intervention, and mitigate the risks and consequences. A failure to incorporate these into your risk programs can lead to disruptions in productivity, morale, and the bottom-line.

$2.9 M

Total Incurred Claims Dollars in 2020 for Workers Compensation [1]

$4,737

Average total incurred Workers Compensation claim amount [1]

60%

Workers want to work in a remote capacity indefinitely [2]

Sources:

[1]The Hartford internal claims data – 2021
[2] LiveCareer survey - 2021

Planning for Each Type of Location

The "curbside" phenomenon touched many service industries as variations of a curbside experience occurs while consumers stay in their car for optimum social distancing. Credit union curbside service is often offered by appointment for member services such as account/loan document signing, pick-up / drop-off, notary services, certificate renewals, and replacement plastic cards.

In addition, branch offices operating with remote employees, drive-thru lanes, and ATMs took on a more significant role in 2020.

It is critical to have a plan to minimize risks with operational change.

- **Slips Trip and Fall claims** (47% frequency / 60% claim dollars) are the most frequent workplace safety loss at credit unions (2016-2020 internal claims data, The Hartford).
- **"Double duty" or "job duties as assigned"** such as moving carpets, shoveling and clearing walkways, handling trash, cleaning & sanitizing, etc. Unfortunately, some of these tasks have also generated unexpected claims.
- **Personal protection and safety measures** for employees should be followed including wearing a face covering, properly washing / sanitizing hands, and appropriate physical distancing.
- **Robbery** can also be a significant exposure especially if the credit union is allowing curbside cash transactions. It is important that the member be vetted when making an appointment by obtaining the vehicle information and license plate. Consider limiting cash transaction amounts and have the member make multiple appointments if a larger cash amount is needed.

  An increase in robberies have also occurred at **drive-thru lanes** and through **ATM attacks** due to the increased use and dollar amounts.

Internal Controls in a Remote Environment

Credit unions have been adjusting their operations and business practices to fit the environment in which they now operate. For many, this meant instituting more flexible work arrangements.

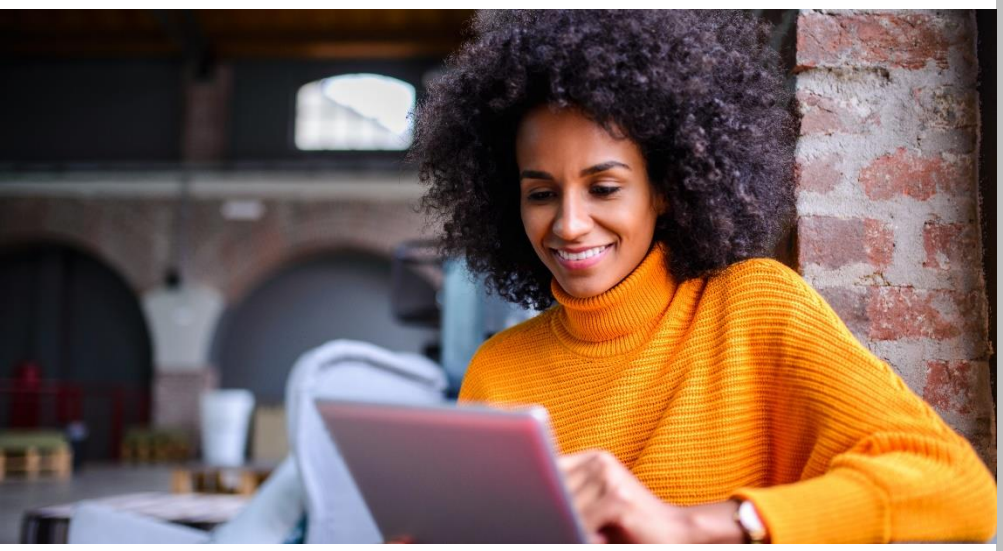
Functional areas involving cash, negotiable items, plastic cards, lending, accounts payable, payroll, and reports accessibility can be impacted if internal controls are not adjusted accordingly.

For more insights…review Flexible / Hybrid Work Arrangements Risk Overview & Checklist.

Physical Asset Management & Remote Work

In order to accommodate employees in this new remote work setting, equipment, supplies, and records made its way out of the office. Items that may have left branch locations include electronic devices (laptops, monitors, web cameras, printers, tablets, phones), furniture (chairs, tables, screen risers, desk lamps), office supplies, and possibly paper documents.

Unfortunately, not everyone always maintained an accurate record of the items provided for remote use.



Trending…Pandemic Fatigue

The pandemic has also introduced a new wave of anxiety. Employees are worried about getting sick, taking care of loved ones, childcare and schooling concerns, job stability, and the prospect of unemployment.

Past incidents have taught us that some perpetrators of workplace violence often struggle with factors like financial setbacks, untreated mental health issues, or domestic violence. Employers have a unique role to play when supporting their employees who may face violence in the home.

Key Takeaway: Expect employees to have different comfort levels in their new work environments, so sensitivity and communication will contribute greatly to their comfort as employees transition back into offices. And, keep in mind, that many team members may have also grown accustomed to the benefits of working from home and may struggle with the necessary adjustments to function in a more rigid office environment.

It can impact your members and office visitors in the same way. While you expect appropriate and courteous conduct in interactions, providing reminders or tips on how to handle negative situations can help ensure the safety of employees from abusive behaviors.

EXPLOITING REMOTE WORKERS

Fraudsters jumped on the opportunity to exploit weak security measures as employees adjusted to remote working environments. By using fraudulent instruction or a Business Email Compromise (BEC) scam, fraudsters request payments – typically wire transfers - through spoofed email to pay vendors under the guise of executive management.

According to Beazley Breach Solutions, there was been a 96% increase in loss frequency and a 950% increase in loss dollars paid to credit unions related to business email compromise.

Credit union staff working remotely are ideal targets for fraudsters as the employees may not be familiar with proper security protocols or may be lax in following procedures.

Additionally, fraudsters may use the excuse of the pandemic to urge staff to make payments they would not normally perform.

A business email compromise scam typically involves an executive level employee's email that has been compromised or spoofed through a phishing attack. The fraudsters create an email appearing to be sent from the executive's email to another individual within the organization requesting a payment – typically wire transfer – or purchase of gift cards.

Red flags to be on the lookout for:

- Urgency of the message
- Request to keep transaction confidential
- Communication only through email and refuses other communication channels
- Requests to change or modify direct deposit information
- Requests for payments to be made to a different account since they are inaccessible due to the pandemic

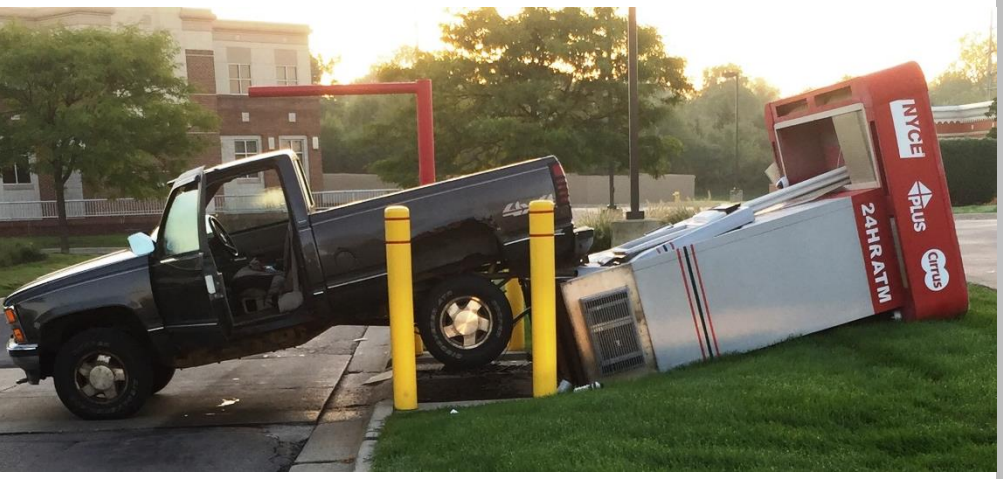
Automated Teller Machines

Automated Teller Machines (ATM) and Interactive Teller Machines (ITM) are part of your members' digital culture and are a big 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; however, they can also introduce an element of risk.

New attacks, largely physical in nature, have been migrating to the United States from overseas.

"Credit unions need to be aware of these attacks — from jackpotting and bust-outs to the smash & grabs of entire machines — and implement solutions to mitigate these risks. The ATM is a convenient channel for everyone including criminals and fraudsters."

Michael Petrone
Risk Consultant - CUNA Mutual Group



ATM Smash & Grab Crimes

These aggressive attacks are comprised of several common traits where the perpetrators typically use stolen heavy-duty trucks with chains or construction type vehicles to rip apart the ATM and gain access to cash canisters. Smash & grab style of attacks rose to prominence in Texas but has migrated to other parts of the country.

Criminals have also become more sophisticated by employing the use of explosives. This has limited the actual time of attack to sometimes just 2 – 3 minutes for cash supplies to be accessed.

As many credit union lobbies have been closed or restricted during the pandemic, members have become much more dependent on ATMs and Interactive Teller Machines (ITMs) to conduct transactions. **Machines located on the outermost drive-thru lane or standalone on an island may be the most vulnerable.**

The damage, or in some cases, destruction of these machines can affect operations as it may take weeks and significant financial resources before they can be repaired or replaced. Property and machine damage costs range between $50,000 to $100,000.

ATM SAFEGUARDS

Consider these loss controls:

- Ensure basic security measures are in place. ATM and ITM machines should be properly secured with bolts into concrete when available and areas surrounding ATMs should remain well-lit with adequate surveillance coverage.
- Implement the use of bollards and barriers. The vehicles typically used in these attacks require adequate spacing to execute this crime.
- Connect with your ATM and ITM providers to inquire about any physical security enhancements that may be available for your existing machines. Certain providers have made enhancements like fortified barriers, door and gate kits, exterior anchor devices, as well as GPS tracking devices available to track compromised currency cassettes. Alarm and sensor upgrades such as high-speed notification to law enforcement or monitoring stations as well loud audible alarms may also be considered.
- Reevaluate currency replenishment schedules and limit cash amounts. In many cases, criminals were monitoring the credit union to identify when the attack would be most lucrative. Varying replenishment schedules and limiting currency amounts are highly advisable.
- In addition to having the ATM connected into your alarm system; consider an audio and/or strobe/flashing light to minimize burglary risk.

It is imperative to exercise prudent judgement in selecting ATM/ITM equipment, location, and security that will provide the greatest degree of protection.

Use this ATM Inspection Checklist and the Currency & Vault Specifications / Storage & Transportation Guidelines to aid your efforts in managing risks associated with security, compliance, tampering, and fraud attempts.

Fraudsters are crafty, knowing how to pressure people to make decisions on the spot by using innovative schemes. Their multi-channel approach looks for victims who find their stories convincing and will willingly share sensitive information, which can be used to authorize and transact many types of transactions. Unfortunately, the fraudulent transaction is often a legit exchange based upon a fairy tale.

81%

first party synthetic, or a real consumer is using an SSN that doesn't belong to them[1]

19%

third party synthetic, which is a totally fabricated identity[1]

[1]Synthetic Fraud and Credit Unions, SentiLink, 2020

Synthetic Identity Theft

Fake consumers, or "synthetic identities," obtain countless deposit accounts, credit card accounts, auto loans, and personal loans costing credit unions hundreds of millions of dollars each year in losses.

81% of synthetic fraud at credit unions is first party synthetic, or a real consumer is using an SSN that doesn't belong to them. When undetected, credit unions typically pull the wrong credit report and inaccurately assess the risk associated with the consumer. The remaining **19% of synthetic fraud is third party synthetic, which is a totally fabricated identity** typically created by organized crime. (Synthetic Fraud and Credit Unions, SentiLink, 2020)

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

Credit Privacy Numbers

In some cases, the SSN used for a synthetic identity is a Credit Privacy Number (CPN). A CPN is a nine-digit number that resembles a social security number, typically provided by a credit repair company. Not all credit repair companies are reputable and promise consumers with poor credit a fresh start by using a CPN. They fail to inform consumers that misrepresenting a social security number on a credit application is a federal crime.

Global Events Make Us Attractive Targets

The pandemic has been a windfall for fraudsters as they exploit the global thirst for knowledge on COVID-19 and the vaccine. Phishing attacks to deliver malware – typically credential-stealing banking Trojans – have been launched to represent the Centers for Disease Control, the World Health Organization, along with fake websites to deploy scams involving fake charities, federal stimulus package payments, and vaccines.

As the **use of mobile banking apps surged during the Pandemic**, so did the risk, warns the FBI's Internet Crime Complaint Center (IC3).

Fake banking apps try to convince you that they are the real deal. Once installed and launched, they lead with a login form and the credentials submitted into the form are harvested.

Members' HELOCs Used to Fund Counterfeit Checks

Home Equity Lines of Credit (HELOC)-related fraud can lead to large losses and are relatively easy to execute by using stolen personally identifiable information (PII). Many cases involve fraudsters – impersonating members – social engineering call center employees into providing a copy of a canceled HELOC check. Losses from a single counterfeit HELOC check have ranged from $30,000 to $350,000.

Recorded mortgages, including HELOCs, are normally public records which allows fraudsters to search for open HELOCs. Once found, the records typically have borrower signatures and account numbers which the fraudsters capture for later use in committing fraud.

Case Study: A fraudster social engineered a call center employee into changing a member's address and phone number. The fraudster social engineered the call center again two days later to reset the member's online banking password. This allowed the fraudster to login to the member's account to order share drafts which were delivered to the new address. The fraudster forged three share drafts totaling $407,000 and funded them through unauthorized advances against the member's HELOC through online banking.

Business Email Compromise

Cybercriminals have gone to great lengths to commit theft or fraud by manipulating credit union executives, employees, and even business members using fake, spoofed, or doctored emails, calls, and even deepfakes or digitally-altered recordings. The surge of business email compromise (BEC) and fraudulent instruction scams typically request large wire transfers. These urgent requests often exceed $1 million.

Both fraudulent instruction and business email compromise scams often focus the request as "urgent" or "pay immediately" in hopes that the employee does not take time to scrutinize the request.

According to Beazley, an increase in these scam-related losses coincides with the increase in remote working, suggesting that detecting and preventing social engineering scams has become more difficult with an increase in distractions.

Mortgage Closings Targeted in Fraudulent Instruction Scams

Prior to a loan closing, fraudsters posing as the title company / closing agent send spoofed emails to credit union / lenders or member / purchasers containing "updated wire instructions."

These "updated wire instructions" are bogus and are intended to have funds sent to an account under the fraudsters control. Loss impact for these have been in the millions!

Business Account Check Kiting

With business revenues plummeting due to the recent pandemic, some businesses have resorted to check kiting to keep the business afloat.

Kiting can lead to enormous account balances on paper and a loss for the credit union when the kite eventually collapses. In fact, check kiting is considered the largest loss exposure associated with any share draft/checking account program.

Losses from check kiting - particularly business kiting schemes - can threaten the solvency of a credit union as the losses can be in the millions of dollars. In fact, two credit unions recently reported kiting losses in excess of $2 million involving business accounts.

ACH Booster Payments

- Similar to check kiting, fraudulent payments are made via ACH debits towards line-of-credit loans (e.g., credit cards) to free up a member's credit limit.
- Member uses up the credit limit before ACH debits are returned unpaid.
- Payments are frequent – several ACH payments are made in a single billing cycle.
- Frequency and amounts grow over time to make up for ACH debit entries that are returned.
- Most payments are returned as NSF or account not found; others returned as unauthorized.
- The problem is not spotted until its too late - when the balance is well in excess of the approved credit limit.

Members continue to be targeted in the Zelle / P2P fraud scam to provide online banking usernames and passcodes or debit card details. This results in unauthorized electronic fund transfers from member accounts via Zelle / P2P. Some credit unions do not intend to re-credit members victimized in this scam because they voluntarily provided the fraudsters with their login credentials or debit card information. Refusing to re-credit members victimized in this scam may violate Reg E.

Peer-to-Peer (P2P) Scams

Fraudsters continue to target members of credit unions offering **P2P like Zelle** by using a sophisticated scam to defeat 2-step authentication which leverages the use of one-time passcodes.

- Fraudsters send text alerts to members – appearing to come from the credit union – warning members of suspicious debit card transactions.
- Fraudsters call those members who respond to the text - spoofing the credit union's phone number - and claim to be from the credit union's fraud department.
- To verify the identity of the member, the fraudster asks for the member's online banking username and tells them they will receive a passcode via text or email and the member must provide it to the fraudster. In reality, the fraudster initiates a transaction, such as the forgot password feature, that generates a 2-step authentication passcode which is delivered to the member.
- The member provides the passcode to the fraudster who uses it to log in to the member's account using a device not recognized by the host system.
- Upon logging into the accounts, fraudsters change the online banking passwords and then use Zelle to transfer funds to others.

P2P Is Changing The Way We Handle Our Money

Splitting any type of bill with a group of friends was a hassle. P2P payments make it easier than ever for consumers to transfer money immediately upon an "IOU." These payments allow the transfer of funds between two parties using their individual checking accounts / debit cards or credit cards through an online or mobile app. However, these measures aren't foolproof. Many P2P systems have been targeted by hackers and scammers.

Reg E & the Zelle / P2P Fraud

Some credit unions have reported that they do not intend to re-credit members impacted by this scam under Reg E's error resolution procedures since the members voluntarily provided the fraudsters with their login credentials or debit card details. Members victimized by this scam are entitled to protection under Reg E due to the transaction being authorized.

§1005.2(m) defines an unauthorized electronic fund transfer as "an electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit." The commentary to §1005.2(m) clarifies that "an unauthorized EFT includes a transfer initiated by a person who obtained the access device from the consumer through robbery or fraud."

Some credit unions may refuse to re-credit members victimized by this scam if the members fail to report the unauthorized EFTs within 60 days of the statement being made available on which the first unauthorized transfers appear. This is a misinterpretation of Reg E. The credit union is liable for the initial unauthorized EFTs even when notification is outside of the 60-day timeframe. The 60-day timeframe is in place for subsequent unauthorized transfers that could have been prevented had the credit union been notified about the initial transaction in a timely manner. Refer to §1005.6(b)(3), which states:

> A consumer must report an unauthorized electronic fund transfer that appears on a periodic statement within 60 days of the financial institution's transmittal of the statement to avoid liability for subsequent transfers. If the consumer fails to do so, the consumer's liability shall not exceed the amount of the unauthorized transfers that occur after the close of the 60 days and before notice to the institution, and that the institution establishes would not have occurred had the consumer notified the institution within the 60-day period.

Internal controls are an integral part of all credit union operations. Unfortunately, dishonest employees and directors cost credit unions millions of dollars each year and consistently top the list of credit union bond losses. These losses tend to surge during and following down financial times or a recession.

Bond claims dollars paid connected to Employee or Director Dishonesty and Faithful Performance [1]

[1] CUMIS Insurance Society, Inc. 2016-20 Internal Claims data

Losses occurred due to the lack of internal controls [2]

19% lack of management review

14% override of existing controls

[2] 2020 Report to the Nations On Occupational Fraud and Abuse, Association of Certified Fraud Examiners

Know what to look for by recognizing the employee behavioral red flags displayed by fraud perpetrators can help detect fraud and mitigate losses.

Don't take matters solely into your own hands by reprimanding and not reporting employee wrongdoing to your bond provider. Check out Unreported Prior Acts.

"In some ways, rapidly redeploying credit union staff to a virtual environment may make oversight and controls more digitized, but it may also uncover new employee & director dishonesty vulnerabilities."

Jay Isaacson
VP, P&C Solutions
CUNA Mutual Group

Common Risk Themes

Mysterious Disappearances of Cash

Disappearance of cash often occurs when clear accountability doesn't exist. Detecting these losses can be difficult. The median duration of fraud schemes is 14+ months.[2]

Expense / General Ledger Fraud

Expense transactions that are not properly segregated or monitored, open you to increased risk. By falsifying numbers associated with purchase orders, suspense accounts and not performing reconciliations, employees have an easy avenue to commit fraud.

Member Account Manipulation

Whether it's manipulating credit union account information or selling member information to outside parties, employees can attack member account funds – often through dormant / inactive accounts.

Fictitious / Unauthorized Loans

Originating fictitious or unauthorized loans, changing existing loan details, or making credit advances for their own benefit are most common. As you expand loan programs, the need for continuous risk monitoring increases.

Funds Transfer Theft

Large sums of money can disappear quickly if proper controls aren't in place to prevent employees from performing the entire funds transfer process. And, once those funds leave the credit union, they often can't be successfully retrieved.

Often Overlooked Controls

- Limiting system access and capabilities
- Performing frequent, regular report reviews
- Segregating duties that restrict the ability for one employee to perform an entire transaction (critical with remote staffing)
- Developing and updating written policies and procedures
- Requiring training of all staff

Human capital management has been redefined and became even more visible during the pandemic. The way we manage and communicate with employees – along with understanding what they value – has shifted and presents various opportunities for success and disruption.

Recruiting a More Diverse, Equitable, and Inclusive Workforce

Embracing differences and working to develop a risk culture and inclusive workplace should be at the heart of today's business. Leveraging different backgrounds, skills, knowledge, and perspectives can enhance your organization's strength.

Credit union leaders have the power to create an open and collaborative atmosphere. Redesigning jobs should be viewed not as an end goal, but as a process that enables work itself to be redefined so that the workforce creates new value.

Finding someone to fit perfectly into a position can be daunting. Whether you're bringing back furloughed employees, refilling positions that had to be reduced, or boosting staffing to cover important roles, it is critical that you have the right resources to manage through these times of uncertainty.

Remote Work Is Here to Stay

Shifting to remote work and virtual collaboration is one of the biggest changes credit unions have embraced to address the increasing complexity of today's environment. Providing access to online communication tools and collaboration platforms is critical.

Employees Demand More From Employers

Between the public health and economic crises, employees feel that their employers need to be part of the solution. Credit unions have to make a societal difference, especially during times of hardship and social polarization.

Employees expect companies to keep their facilities clean, communicate regularly about their status, and maintain safe working conditions. When job seekers evaluate a job offer, they often choose "safety of the work environment" over "opportunities for professional growth" and even the "quality of potential coworkers."

Flexible or Hybrid Work Arrangements

Flexible or hybrid work arrangements are alternate arrangements or schedules that vary from the traditional work setting. These types of arrangements help employees balance the needs of work and life and the organization can retain key talent in addition to boosting employee satisfaction and productivity.

Unfortunately, poorly adopted flexible work arrangement plans can lead to increased risk around employment practices and management controls. Consider these common risks:

- Privacy and security of your member and credit union information should be a top priority.
- Oversight with remote employees is monitoring and tracking the hours they are working outside of the office – especially those who aren't salaried and are non-exempt. Fair Labor Standards Act (FLSA) violations could apply if not compensated appropriately.

Pandemic Impact

The pandemic impacts every employer and all members of the public. How you address the pandemic, and the vaccine is of utmost importance. You need to establish clear, written policies, procedures, and employee training to assure compliance.

The perfect storm of challenges in 2020 highlights the importance of deliberate contingency planning. Unfortunately, disasters and threats can occur at any time. Some face considerable financial pressures and feel constrained to make investments to improve resilience in 2021. It is not a "nice to have" but a "must do."

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

Consider these key concepts:

- Cultivate a flexible and resilient culture that can respond to upheaval with a business-as-usual approach.
- Emphasize speed and flexibility so your organization can quickly adapt to rapid change.
- Integrate testing and lessons learned into a continuous improvement program. Identify areas that need improvement, and address and correct shortcomings highlighted in after-action reports.
- Assess the organization's reliance on third-party service providers and identify alternatives in case of loss of these providers.
- Evaluate work digitization to ensure that employees can access what they need remotely.
- Ensure that resiliency planning accounts for the portion of the workforce who may continue working remotely.

Having the Right Plan In Place

Many found that they were missing an adequate Business Resiliency Plan opting in favor of Disaster Recovery or Incident Response Plans. Those are both important elements of continuity but are not always adequate to help minimize operational risks and reduce business disruption while maintaining a strategic perspective on the future.

Some of the most evident and challenging components were:

- Velocity and duration of threat
- Plans did not address major issues which were peripheral to work, including home schooling, at-risk relatives, and the psychological effect of working remotely.
- Often only one location being uninhabitable was considered, and not all locations due to Federal, state and local government orders
- Employee supply and equipment needs for a home office environment was lacking

Invest in a business resiliency program that is ongoing and continuous. Review the Business Resilience Planning Guide & Checklist.

More Frequent Plan Visits

Before the pandemic, it was not unusual for business continuity teams to review and update plans once a year. However, in response to the pandemic many teams share data weekly or even daily to continuously monitor an evolving and highly uncertain environment. The good news is that the pandemic reinvigorated the need for credit unions to imagine extreme scenarios and planning.

Consider Concurrent Threats

Business continuity management must address multiple concurrent threats now more than ever. Simultaneous natural disasters, widespread power or technology outages, civil or political unrest, and other events could conceivably threaten business operations on a large scale. The potential convergence of disaster events requires risk management functions to ask new questions, such as:

- What key infrastructure should be in place to address compounding disaster events and ensure resilient enterprise operations?
- Can remote workers perform their work as multiple disaster events occur simultaneously?
- Have we thoroughly conducted an evaluation of third-party service providers that contribute to critical business services?

Offering lending products is the backbone for many credit unions. A variety of consumer protection and collection laws and regulations (i.e., TCPA, FDCPA, FCRA, UDAAP, etc.) apply when a loan becomes delinquent and goes into collection. Mistakes by the loan officer or collection staff can result in legal liabilities and damage to the credit union's reputation.

Loan Servicing & Collections

Members and small businesses may suffer from prolonged unemployment and the inability to make payments – making loan servicing and collections even more critical.

2021 will likely be characterized by lower income, impairment of asset quality and reduction of reserves. This can be a challenging time for credit unions and may increase the possibility of consolidations for credit unions with marginal net worth.

Comparable to the credit crisis of 2009-2011, you should continue to carefully serve members while other financial institutions pull back in their lending. Credit unions have the opportunity to restructure loans and find ways to help members while seeing increased membership growth and savings dollars as members reward accommodation with loyalty.

Be sure to stay on top of changing risk profiles, especially for those who are experiencing hardship and could potentially become delinquent – even if they had no past delinquency history. Some members may accept deferments or forbearance, even if they have suffered no disruption of income. In other words, they may be holding on to cash because they are not sure what to expect or how long it will take for the economy to fully recover.

Maintaining an empathetic approach to member relations in collections will likely help during and after the pandemic.

Notice of Disposition and/or Notices of Deficiency

Plaintiff attorneys continue to be successful with class action lawsuits against credit unions due to deficiencies in collection letters. Specifically, Notice of Disposition (commonly referred to as notices of intent to sell collateral) and Notice of Deficiency sent after the collateral has been sold are the letters / notices targeted. Lack of detail in these notices is being scrutinized. These lawsuits have been going on for several years with credit unions being required to waive remaining deficiency balances, return payments toward deficiency balances, return 10% of the principal amount of the original debt, and pay statutory damages.

Recent lawsuits have included several of the usual claims alleging the Notices of Disposition:

- Do not state the borrowers have a right to redeem the collateral until it is sold;
- Do not inform the borrowers they have a liability for a potential deficiency balance;
- Do not inform the borrowers they may attend a public sale and bring bidders.

A newer allegation claims a Notice of Disposition lists the charge for an accounting as a higher amount than allowed for that state.

Review Collection Letter Litigation Risk Overview within the Protection Response Center.

Telephone Consumer Protection Act (TCPA)

While TCPA litigation is often centered around telemarketing calls and texts to members without first gaining prior express written consent, outgoing calls or texts related to collections, servicing or fraud alerts when made without the appropriate prior express consent can also pose risks.

Lawsuits against credit unions have most recently involved:

- calls / texts to members' cell phones to collect delinquent loans or negative deposit account balances using an automatic telephone dialing system (ATDS) or a prerecorded/artificial voice without obtaining the requisite prior express consent of the member.
- third-party debt collectors retained to collect debt on behalf of the credit union. Credit unions can be held liable for the vendor's failure to comply with the TCPA.

Review Telephone Consumer Protection Act Risk Overview.

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

Using analytics to support strategy & control losses

The key is to combine existing data with **artificial intelligence (AI) and machine learning tools**, and skilled analytics to reveal member trends, behaviors and expectations down to an individual level. These insights allow you to deliver relevant, personalized offers and experiences that are valuable to the member, unique to your credit union, and differentiated from your competition.

Account Opening / Loan Evaluation: Validate the authenticity of applicant info to improve accuracy and efficiency.

Payment Authorization: Evaluate requests and authorize payments in real-time.

Improved Fraud Prevention: Reduce manual review 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

Digital Lending

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.

Consumer Behavior

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.

Credit union members have adapted to a more remote world by drastically changing how they buy products and approach financial transactions. Most experts see the impact on financial institutions as an acceleration of the existing trend toward more mobile banking and less branch banking.

Credit unions were already well along the digital and mobile journey with members but accelerated implementation to serve members during lock-downs and shelter-in-place requirements.

Reducing Friction

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 virtual experience while you provide transaction security.

Full integration means the ability to switch methods of engagement, i.e., from a mobile device to a branch or call center. It is important to require member authentication and validation at each layer of the digital channel and transaction.

The riskiest 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. While focusing on streamlining the loan process can create an elevated member experience, it can also make it easier for fraudsters to cheat the system.

2020 prompted a slowdown in merger activity primarily due to economic uncertainty and operational issues. There are several variables impacting credit unions, including: unemployment, income stability, and consumer spending. In order to pursue a well-structured, strategic merger and acquisition plan, you'll want to mitigate potential issues and challenges.

Oversight and Communication

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.

Member communication can be the difference between a successful merger and a chaotic one.

- Follow federal and state timelines regarding merger communication, including member groups, regulators, and media.
- Share the announcement to both membership bases at the same time and maintain consistent, frequent updates on merger progress and important timelines.

Pandemic Impact

The pandemic-induced recession will increase the severity of loan losses. When acquiring credit unions or other financial institutions, you should be cautious about the pandemic impact on credit quality.

Expect merger and acquisition activity to resume in late 2021. Credit unions hardest hit by the pandemic will likely be the potential targets.

Importance of 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 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 interview 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.

Expect the Unexpected

Strategic decisions should be carefully considered to ensure that hidden costs and risks are properly identified and analyzed. Be aware of redundant systems, assets, lasting contracts, applications and processes. The pandemic will have a lasting impact on how some deals get done, so be creative to determine what you can do now and what needs to change.

Compliance risk has become a significant ongoing concern for financial institutions. In addition, establishing compliant operations can be challenging by increasing the cost of service and sometimes making the delivery of great member experience more difficult. Credit unions face expanded expectations that can lead to higher costs and losses from escalating litigation, penalties, and staffing needs.

Strengthening Controls Over Access To Sensitive Data

Regulators have been ratcheting up enforcement activity under data protection laws implemented over the past few years.

In addition, many expect the new administration to focus more on consumer protection in regulation and enforcement actions across the business landscape, and this will likely extend to cybersecurity and data protection practices as well.

With a broadening push to offer more proof of compliance to industry regulations and requirements, with clear ways for consumers to validate you are doing what you say you're going to do; it is critical to allocate time and resources to comply:

- Build and review holistic, risk-based privacy programs.
- Data mapping and inventories are first step, so you know who has and should have access to what; and how that access being used and being controlled.
- Align with other cross-functional programs – data governance, cybersecurity, third-party risk management, compliance.
- Follow or incorporate privacy framework developments (e.g., NIST).
- Educate and learn from your privacy stakeholders – IT, marketing, operations, security, etc.
- Watch regulatory developments, data security litigation, and AG enforcement closely. Pay attention to state and federal proposals.

Failing to Refund Unearned GAP Fees

There has been a recent increase in class action litigation directed toward indirect loans that were originated by automobile dealers on retail installment sales contracts (RISC). The allegations accuse creditors of failing to process refunds when a Guaranteed Asset Protection (GAP) Waiver terminates early, which may include:

- Loan payoff prior to maturity, including sale or trade of vehicle
- Repossession and disposition of vehicle
- Customer cancellation of the GAP Waiver

Overdraft / NSF Fee Litigation

Overdraft / NSF fees continue to be a sore spot for consumers. In fact, consumer advocacy groups have targeted overdraft programs – often referred to as courtesy pay or overdraft privilege programs – and the disproportionate impact the programs have on certain consumers.

Recent lawsuits alleged credit unions:

- Improperly charged overdraft fees on debit card transactions because funds were previously "set aside" during the preauthorization hold process. There may have been an intervening debit after the preauthorization hold was placed that reduced the available balance so that when the debit card transaction posts, it takes the account negative resulting in an overdraft fee.
- Credit unions improperly charged multiple NSF fees on the same transactions. This typically involves the submission of ACH debits to member accounts that are returned unpaid due to insufficient funds. The ACH rules allow the payees to resubmit the ACH debits for payment up to 2 times. The debits would be returned again if there are insufficient funds in the account resulting in additional NSF fees.

Past lawsuits alleged that overdraft fees were improperly charged using the "available" balance rather than the "actual" or ledger balance because in many situations, the actual balance was sufficient to cover the debit. Additionally, they alleged that financial institutions resequenced debits from highest dollar to lowest dollar which used up the available balance much faster resulting in excessive overdraft fees.

Patent Infringement

Several credit unions have received letters from counsel representing **BioCrypt Access, LLC** suggesting that they may be infringing on several patents that cover many applications and devices in the biometric identification and access space commonly used in mobile / digital banking apps . BioCrypt counsel invites the credit unions to enter into a non-exclusive license to BioCrypt's patents. See related RISK Alert re: BioCrypt.

Caselas, LLC has been filing lawsuits against credit unions alleging infringement on patented technology used in connection with payment card processing that is designed to help to minimize the risk of merchant chargebacks. See related RISK Alert re: Caselas.

Some organizations have been known to file lawsuits in some states against both banks and credit unions alleging infringement on multiple patents.

Action Steps to Consider

Credit unions should review their technology vendors licensing agreement and/or professional services agreement to ensure it contains a provision to defend, indemnify and/or hold the credit union harmless from damages the credit union may incur from alleged patent infringement claims.

The licensing and/or professional services agreement may contain a deadline for notifying the vendor when the credit union receives notice of alleged patent infringement, and failure to provide notice within the specified timeframe could result in the credit union waiving its rights to be indemnified.

TCPA Relief for Credit Unions?

The Supreme Court, on April 1, 2021, adopted a narrow interpretation of what constitutes an automatic telephone dialing system (ATDS or autodialer) under the Telephone Consumer Protection Act (TCPA). It is viewed as an important decision for credit unions; however, the Supreme Court did not address what it means for the equipment to have the "capacity" to generate random and sequential numbers

The Supreme Court overturned a Ninth Circuit decision that broadly defined an autodialer as any equipment that has the capacity to store and dial numbers, regardless of whether those numbers were generated by a random or sequential number generator. The Supreme Court held that to qualify as an autodialer under the TCPA, the equipment must have the capacity either to store a telephone number using a random or sequential number generator or to produce a telephone number using a random or sequential number generator.

However, the Supreme Court did not address what it means for the equipment to have the "capacity" to generate random or sequential numbers. In other words, the decision did not directly address the question of whether an autodialer includes equipment that has but does not use, or equipment that can be updated or modified to have, the ability to store or produce numbers using a random or sequential number generator.

Business changed in 2020 — as did your personal threat model. It also introduced underappreciated burdens as well, such as preserving security when home becomes work, and ensuring we manage risks even as individuals out of the office. Keeping ahead of the complex array of ever-changing risks, compliance issues, and industry regulations that are impacting credit unions requires keen awareness, effective preparation, and loss control scrutiny.

When risk management is effective, typically nothing bad happens. But, if you're blindsided by a problem, your credit union reputation takes the hit. Don't let not knowing which emerging risks are around the corner take the blame.

While each credit union has its own unique risk footprint, this **Emerging Risks Outlook for 2021** introduces risks and trends that most likely should be on your radar to assist you in rethinking your protection.

*If you'd like to discuss any of these risks in more detail, simply schedule a no-cost personalized discussion with a CUNA Mutual Group Risk Consultant or contact us at riskconsultant@cunamutual.com or at **800.637.2676**.*