

Business Protection Resource Center (BPRC)

User guide



With easy access to actionable, educational insights, relevant resources, and proven risk mitigation guidance, you can rise above your risk. The **Business Protection Resource Center** is a one-stop online shop for your emerging risk needs – RISK Alerts; loss prevention resources and checklists; on-demand training; and virtual events.

www.trustage.com/bprc

You'll also have access to additional partner resources related to cybersecurity, employment practices, and workplace safety/wellness. In addition, use the online forms to easily report a risk/scam, ask a question, or schedule a 1:1 discussion with a TruStage™ Risk Consultant at riskconsultant@trustage.com or **800.637.2676**.

Getting access to the Business Protection Resource Center

1. Go to www.trustage.com
2. Click **Log in** in upper right-hand corner
3. Select **Sign in to your business account**
4. Select **My Services for credit unions**
5. Enter your User ID and password. Complete authentication steps
6. If you already have a User ID and password, Click on your name in the upper right corner and then click **Edit services and roles**
7. Scroll down to the Credit Union Protection section and check **Protection Resource Center**
8. Click **Submit** at the bottom of the page

If you do not have a My Services account, after Step 2 above, select **Create new account**. Follow the prompts and enter your information to create a new account. Once the account is created, click **Manage my services** and return to step 7 above to request access to the Protection Resource Center.

Not receiving RISK Alerts or event invites

1. After signing in and accessing My Services for credit unions, click on your name in the upper right corner and then click **Edit profile**
2. From the Edit profile page, click **Edit Subscriptions**
3. Select **RISK Alerts** and **Risk and Compliance Webinars** from the Credit Union Protection section
4. Click **Submit**

RISK Alerts

RISK Alerts highlight emerging risks or prevalent scams occurring within the financial services industry. Each Alert provides risk details, recommended action steps, and links to related resources. On average, 60 RISK Alerts are distributed annually to a RISK Alert subscriber list of ~17,000 credit union professionals from TruStage bond policyholders.

RISK Alerts are distributed via email and published within the Business Protection Resource Center and the RISK Alerts Library.

RISK Alert types

- **Warning** - Just-in-time risk or immediate issue risks that have become more prevalent and are impacting credit unions.
- **Watch** - Risk conditions are right to impact credit unions as time goes on. Corporate Check Fraud Alerts (content shared by policyholders) are also distributed as a Watch.
- **Awareness** - Risk awareness/education on a risk topic.

RISK Alert email

- Click < **Access full alerts & resources** > to open the Alert within the BPRC (User ID/Password required)
- Click < **Download PDF** > to open the Alert. The PDF version from the email is only accessible for 30 days.

Benefits of accessing RISK Alerts via BPRC

- No limit on accessibility
- Easy access to related resources
- Ability to review additional, previously-issued RISK Alerts on the specific topic
- Sorting and filtering capabilities within the RISK Alerts library
- Ability to access when the risk is most relevant for your organization

Stay on top of emerging risks [View in browser](#)

TruStage

Actionable insights for bond policyholders

[Access full alerts & resources](#)

Awareness **Watch** **Warning**

Credit unions experience losses associated with VIN cloning

VIN cloning happens when a Vehicle Identification Number (VIN) is stolen from a legitimate vehicle and attached to another vehicle, which is typically stolen. This fraudulent practice conceals the real VIN of the stolen vehicle, essentially giving it a fake ID. The result is two cars on the road with the same VIN.

[Download PDF](#)

Ask our risk consultants
Discuss how to identify risk, mitigate losses, and receive insightful resources and tested practices. [Ask us, we have answers](#)

Keep ahead of emerging risks
Risk management virtual events focus on risk insights and loss trends impacting credit unions just like yours. [View our 2024 schedule](#)

TruStage

TruStage

RISK Alert

Actionable insights for bond policyholders

Awareness **Watch** **Warning**

Credit unions experience losses associated with VIN cloning

VIN cloning happens when a Vehicle Identification Number (VIN) is stolen from a legitimate vehicle and attached to another vehicle, which is typically stolen. This fraudulent practice conceals the real VIN of the stolen vehicle, essentially giving it a fake ID. The result is two cars on the road with the same VIN.

Alert details

The VIN, or Vehicle Identification Number, is the unique identifier assigned to every car when it's manufactured. It is significant because it contains all the essential information about the make, model, year of production, manufacturing location, and more. Think of it as the car's fingerprint; no two vehicles legitimately have the same VIN.

VIN cloning is primarily done to mask the VIN of a stolen car, typically with the VIN of a different car from another region. Doing this makes it difficult for law enforcement officials to trace the vehicle back its rightful owner.

How does it work?

A criminal steals a vehicle of the same year, make, and model, to the one with the legitimate VIN. They then, replace the stolen vehicle's true VIN tag with a counterfeit one, turning the stolen vehicle into a clone of the original. From there, the criminal sells the cloned vehicle to an unsuspecting buyer, typically under false pretenses using fake ownership documents.

The practice of VIN cloning is on the rise across the country with CARFAX reporting an increase of 63% from 2019 to 2023.

Risk mitigation

Look for these indicators that a vehicle has been cloned:

- **Gaps or missing vehicle registration information.** Periods of time when there's no registration information reported.
- **The vehicle has been registered in multiple regions.** It seems like the car is "hopping" around from state to state, or country to country in a short window of a few days or weeks.
- **Additional history in other cities.** If a vehicle history report indicates additional damage or history in different locations that doesn't line up with the vehicle's history as presented by the member or dealer.

Date: June 20, 2024

Risk category: Loans; delinquency; collections; notice of deficiency balance; notice of disposition; collateral; climate

States: All

Share with:

- Collections
- Executive management
- Loan manager
- Loan staff
- Risk manager

Facing risk challenges?:
[Schedule](#) a no-cost, personalized discussion with a Risk Consultant to learn more about managing risk.

Finding a RISK Alert

On the Business Protection Resource Center home page, you will find the five most recent RISK Alerts published.

- Scroll down to see these Alerts listed on the center of the Resource Center home page
The list includes RISK Alert title, date published/distributed, a short Alert description, and a link to < **view resource** >
- Click on < **view resource** > to open, review, and print the RISK Alert

To view a complete list of RISK Alerts published < **scroll** > to the bottom of the five most recent Alerts on the Business Protection Resource Center home page

- Click on < **view all RISK Alerts** >
- All RISK Alerts are listed in date order – most recent update listed first. You can also click the < **Title/Date** > toggle within the table to place the Alerts in alpha order

The RISK Alerts library also contains:

- Alert type – Awareness; Watch; or Warning
- Related resource links
- Within the RISK Alerts library, you can:
 - < **Search** > by typing in key words
 - < **Select a resource type** > from the dropdown – RISK Alert is showing
 - < **Select a category** > from the dropdown of 30+ topics
 - < **Select a role** > (e.g., Branch Operations) from the dropdown

Once you make your selections, click on < **Search** > below the filtering categories

Remember to clear your filters by clicking on < **Clear** > after each search

RISK Alerts

CISA warns of ongoing cyber threats to critical infrastructures

RISK Alert

6/25/2024

CISA (Cybersecurity & Infrastructure Security Agency) recently issued an advisory warning of the ongoing threat to critical infrastructure across multiple sectors, including financial institutions. Cyber actors have increased aggressive threats with aims of disruption or destruction of critical services to compromise critical American infrastructure, including FIs in the event of increased geopolitical tensions and/or military conflict with the United States. Credit unions should remain extremely vigilant of cyber risks like the ones warned of by CISA.

[View resource](#)

→ [View all RISK Alerts](#)

RISK Alerts library

[Loss prevention library](#)

[RISK Alerts library](#)

[Webinars and education](#)

[Emerging Risks Outlook](#)

[Risk Management overview](#)

Search

RISK Alert

Select a category

Select a role

→ Search

Clear

Search

ATM

Artificial intelligence

Select a category

Account takeover

ACH fraud

Artificial intelligence

Asset management

ATM

Submitting an idea for a RISK Alert

On the Business Protection Resource Center home page, you can report a risk or scam via an online form.

- Click on < **Report a risk or scam** >
- Enter < **credit union name or TruStage contract number** > within the search field.
- Select the appropriate credit union name from the generated list.
- Complete the Report a RISK Alert form. Click < **Next** > to move through and complete the form.
- On the bottom of the form, click the < **Agree radio button** > to confirm the information entered.
- Click < **Submit** >.
- You'll be prompted to view or download a PDF version of your form containing the information that you've just entered. Click < **View** > to view the PDF or click < **Download** > to download and/or print the PDF.
- Close the PDF to return to the Form Confirmation page.



Search contract number

Name or Contract Number

My Services | Insurance | Claims | Policies | Lending | Support | Training & Webinars

Report a RISK Alert

Upload Documents | User Guide | FAQs | Change Credit Union

REPORT A RISK ALERT
048- | Credit Union | Bradley J
* Required Field Indicator

Contact | Alert Information | Corporate Check Fraud | Review

Contact Information

Please enter the Credit Union (or CUSO) contact information for this RISK Alert form

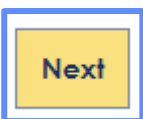
* First Name ⓘ | * Last Name ⓘ
Bradley |

Title ⓘ
|

* Organization Name ⓘ
Credit Union

International Address ⓘ

* Address ⓘ
|



Risk resources

Risk resources – risk overviews, whitepapers, checklists, self-assessments, planning guides - provide an in-depth look at a variety of risk topics. Use these resources to better understand specific risks and mitigation tips that credit unions should consider. These risk resources help build awareness, address critical questions, and drive credit union action to minimize losses.



Fraud & scams

Member risk overview



Each year, fraudsters find new ways to trick people and financial institutions out of money. While some scams involve new tricks, many have been around for decades. Of the over 2.3 million fraud reports, 26% indicated money was lost. In 2022, consumers reported losing nearly \$8.8 billion to fraud.

Fraudsters target the weakest link: humans

Using common channels like emails, text, and phone calls; fraudsters typically disguise their identity while retrieving confidential member information. They use tactics to succeed by tapping at the basic human instincts to trust and please. The scams look to catch your employees off-guard and/or to dupe your members into making security mistakes or giving away sensitive information and money.

No matter the channel, 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 click on links or share sensitive information, which can be used to authorize and transact many types of transactions.

Scams are often hard to detect at a quick glance; however, these common red flags can help. Keep in mind...it is not uncommon for fraudsters to use intimidation tactics and urgent requests.

As fraudsters get more sophisticated in the ways they exploit technology and humans; it is even more important to know what to look for, to take the right action steps, and remain vigilant. We're all human, after all.

You can report fraud, scams, and other illegal business practices by going to the Federal Trade Commission website www.ReportFraud.ftc.gov.

Younger people lost money to fraud more often than older people

43%

Victims ages 20-29 lost money to fraud

23%

Victims ages 70-79 lost money to fraud

However, people aged 70+ had a much higher median loss

Age	20-29	70-79	80+
Loss	\$548	\$1,000	\$1,674

Source: Consumer Sentinel Network Data Book 2022, Federal Trade Commission

Risk overview



Protect your identity & money



Fraudsters continually find new ways to trick innocent people out of money or personal identifiable information. Whether it's an imposter scam – impersonating a credit union employee, a grandchild, debt collector, etc. – or stealing someone's identity, these fraudsters know how to pull it off.

Fraudsters will use several different social engineering techniques to acquire sensitive information such as usernames, passwords, and account or payment card details – all while trying to trick you into believing they are legit:

- Phishing (through email)
- Vishing (through phone calls)
- SMishing (through SMS/text messages)
- Malware (malicious software)

Fraudsters will also spoof the credit union's contact info (phone number, email, etc.) to appear to be from the actual credit union.

Regardless of the fraud type or intention, fraudsters' first objective is to convince others that they are a real member. They often:

- Build victim profiles
- Change members' contact information
- Request wire transfers and withdraw funds
- Request canceled checks
- Order share drafts
- Request password resets
- Request credit/debit cards
- Set-up audio response or online banking
- Compromise login credentials including one-time-pasccodes

Common warning signs

- Don't always trust the display name – criminals will spoof the email name to appear to be a legitimate sender
- Check for misspelled words, bad grammar, and/or typos within the content
- Be cautious of clicking links and opening attachments. Don't click unless you're confident of the sender or expect the attachment
- Asking you to share a one-time passcode sent to your device (when they called you)
- Check the solution - many legitimate businesses will use a personal solution
- Do not provide personal information when asked
- Be suspicious of urgent or immediate response needed or unauthorized login attempt of your account
- Don't believe everything you see: Brand logos, names and addresses may appear legitimate
- The recipient group seems random or unusual (e.g., all last names begin with the same letter)
- The email appears to be a reply to a message that you didn't actually send
- Monitor the sender's email address for suspicious URLs & domains – fraudsters often using similar letters and numbers
- If something seems suspicious; contact that source with a new email or phone call, rather than just hitting reply
- Always, be wary of tempting offers

Member guide

Slip, trip & fall prevention checklist

Use this checklist to help detect and minimize the slip, trip and fall risks.

Location: _____ Date: _____

Inspected by: _____ Photographs attached: Yes No

Condition/Behavior	Acceptable Yes/No	Noted action
General		
No spills or wet floors noted in any area		
"Wet Floor" signs posted as needed		
"Wet Floor" signs removed as soon as floor dries		
No cards noted in walkways. Cards around equipment, & appliances are restrained		
No broken stairs, loose stair coverings / nosing, broken tiles, or other floor defects		
Elevators line up evenly with floors		
No carpet or mat defects - no bunching, curling or buckling		
No throw rugs noted		
Walkways clear. No stored objects in stairways or corridors		
Handrails in stairways present and secure		
No burned out or inoperative lights. Lights are auto on, or quick motion activated (do not require turning on switch)		
Employees required are wearing slip-resistant footwear with closed toes and heels		
Dry mops available near entrances/ dry mopping schedule used during wet weather and in restrooms, etc.		
Indoor walking / working surfaces =4 feet off ground guarded with railing and barricaded or blocked from unauthorized access (e.g., construction areas, mezzanine, roof, or other work platform)		

Checklist/assessment

The best message is often the simplest

Run

Your priority should be to get away from the assailant / shooter.

Hide

If unable to safely evacuate the path of an assailant...fortify your position, avoid detection, and wait for law enforcement.

Fight

As a last resort, and only when your life is in imminent danger, attempt to disrupt the shooter with physical aggression.

Remember:

- Take sound seriously
- Have an escape route and plan in mind
- Proceed to rally point if safe
- Move away from gunfire
- Leave your belongings behind
- Keep hands visible
- Do not attempt to move wounded people
- Avoid elevators
- Run in zig-zag patterns
- Follow the instructions of law enforcement
- Consider alternate escape routes (e.g., windows)

Be sure to:

- Hide in an area out of the assailant's view
- Secure and barricade the door to prevent easy entry
- Turn off lights and avoid casting shadows under the door
- Remain quiet and still
- Silence your cell phone. Dial 911 only when it is safe to do so
- Do not stand directly in front of the door
- Hide behind large objects
- Do not open the door for anyone
- Look for potential weapons
- Spread out in room staying low to ground. Do not huddle.
- Identify a secondary exit (e.g., door or window) so that you can get out if needed

Don't forget:

- Act immediately as firing is critical. The decision to fight is yours and yours alone to make
- Do not go looking for danger. Only fight when the intruder makes contact with you, and you have no other option.
- Act with physical aggression and try to disarm the shooter
- Yell, jump, move your arms
- Overpower the armed aggressor by using strength in numbers
- Throw items and improvising weapons


Proprietary and confidential. Do not distribute. | 3

Employee guide

Finding a risk resource through the Loss prevention library

From the Resource Center home page

- Click on < **Loss prevention library** > from either the left navigation or from the center of the page
- Click on the < **specific risk topic** >
 - Check fraud
 - Compliance/litigation
 - Consumer payments
 - Cybersecurity
 - Deposit account services
 - Disaster preparedness
 - Employment practices
 - Funds transfer/ACH (example shown)
 - Internal controls/governance
 - Lending risks
 - Physical security
 - Workplace safety/wellness

Within the specific risk topic page, you can open, review, and print the resources – e.g., overviews, whitepapers, checklists, related links - within that landing page.

- Click on the specific resource to open the media file
- To access another specific risk topic, simply click on another topic from the navigation on the left
- To return to the Resource Center home page, click on the < **Business Protection Resource Center** > link shown above the page title



TruStage business resources / Business Protection resources / **Business Protection Resource Center** / Loss prevention library / Funds transfer/ACH

Finding a risk resource through the RISK Alerts library

From the Resource Center home page

- Click on < **RISK Alerts library** > from either the left navigation or from the center of the page
- All risk resources and RISK Alerts are listed in date order – most recent update listed first. You can also click the < **Title/Date** > toggle within the table to place the Alerts in alpha order
- Within the RISK Alerts library, you can filter for a resource related to a specific risk topic:
 - < **Search** > by typing in key words
 - < **Select a resource type** > from the dropdown
 - < **Select a category** > from the dropdown of 30+ topics
 - < **Select a role** > (e.g., Branch operations) from the dropdown



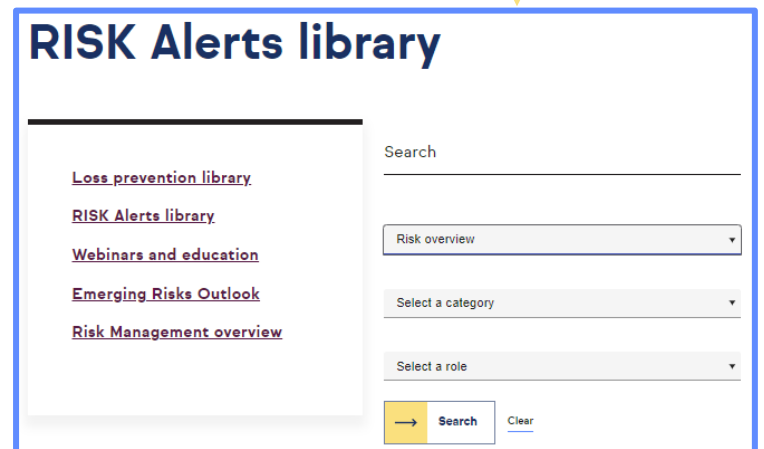
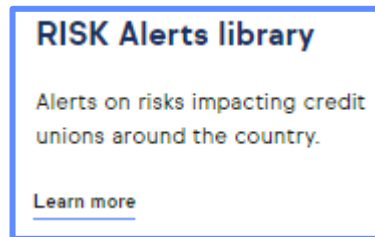
Once you make your selections, click on < **Search** > below the filtering categories

When you've located the risk resource, click on the < **resource title** > to open, review, and/or print the resource

The listing shows the title, type of resource, a short description, and links to related resources.

Remember to clear your filters by clicking on < **Clear** > after each search

To return to the Resource Center home page, click on the < **Business Protection Resource Center** > link shown above the page title



<p>Lending Collections risk overview Alert type: Risk overview Updated: 6/20/2024</p>	<p>Offering lending products is the backbone for many credit unions. You have verified the member and properly determined their eligibility for credit and the ability to repay. When the ability to repay turns into a collection effort, is your credit union prepared to collect the funds, correctly?</p>	<ul style="list-style-type: none"> • Collection letters risks overview • Telephone consumer protection act risk overview
---	---	--

**** As of July 1, 2024, not all risk resources have been added to the RISK Alerts Library. ****

Webinars & education

Risk management virtual events are focused on emerging risks and loss trends impacting credit union organizations. Each session delivers actionable insights, proven guidance, and relevant resources that credit unions can use. These virtual events are exclusively available at no additional cost to TruStage™ bond policyholders.

Registration for live events

Invites are distributed via email to individuals with sign-on access to the Business Protection Response Center; however, you can also register by:

- Click the < **Webinar and education** > link from the left navigation or center of the Resource Center home page
- Choose the upcoming session from those listed and click < **Register now** >
- Complete the registration information
- Click < **Register now** >
- After submitting your registration, you will receive a registration confirmation on the website and via email.
- Click < **Add to calendar** > to ensure the time is reserved on your schedule.

Note: You can only register for the upcoming three events. The live events change monthly.

Webinars and education

Webinars, Office Hours, recordings, and interactive training.

[Learn more](#)

Office Hours: Fraud & Scams

July 24, 1:00 PM CT

→ Register now

Let's start with some basics

First Name*

Last Name*

Email Address*

Title*

Credit Union*

State*

Phone (###) ###-####

Contract Number (###-####-#)

What questions do you have?

→ Register now

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

Executive Vice President
\$3 billion credit union

Your registration is confirmed

Thanks for reserving your spot for Fraud & Scams. Check your inbox for a confirmation email with login instructions.

→ Add to calendar

Webinars & education

Risk management virtual events are focused on emerging risks and loss trends are also available on-demand. These on-demand sessions do not require registration and can be accessed directly within the < **Webinars & education** > section of the Business Protection Resource Center.

Accessing on-demand events

- Click the < **Webinar and education** > link from the left navigation or center of the Resource Center home page
- Scroll to the On-demand webinars & training section of the page
- Select from the categories, then click the < **+ plus sign** > for more info about each on-demand session.
- Each session contains a < **Presentation** > that shares the slide deck and a < **Recording** > which plays the slides and audio for the session.

Webinars and education

Webinars, Office Hours, recordings, and interactive training.

[Learn more](#)

How a traditional P2P/Zelle fraud scam works

1. Members receive account alert via text message appearing to come from credit union - suspicious debit card transactions
2. Fraudsters call members who respond to the text spoofing the credit union's phone number - claims to be from CU fraud department
3. 1. Fraudsters can members into providing usernames (to verify identity)
2. Fraudsters use the "forgot password" feature - triggering a passcode sending it to member's mobile device
4. Fraudsters can members into providing passcodes (to verify member's identity)
5. Fraudsters use passcode to reset member passwords
6. Fraudsters login to member accounts and use Zelle/P2P to transfer funds to others (money mules)

Fraudsters prefer to target P2P platforms like Zelle due to the speed of the payments - minutes versus hours or days - which means instant money.

Some scam tactics used against credit unions that don't offer P2P. Fraudsters deploy tactic to harvest login credentials.

TruStage | Proprietary and confidential. Do not distribute. | 5

Webinar recordings

Account Takeovers & Real-Time Payments +

Account Takeovers & Real-Time Payments ×

[Presentation](#) | [Recording](#)

While real-time payments dramatically improve the speed and efficiency of the U.S. payment system, offering real-time payments will also certainly attract fraudsters. Our TruStage™ Risk Consultants discussed some keys to real-time payments, transaction risks, and account takeovers.

60 minutes / Presented live March 20, 2024 / Deposit Account Services

Other Risk Management resources outside of the Resource Center

Emerging Risks Outlook

While each credit union has its own unique risk footprint, this Emerging Risks Outlook web landing page introduces risks and trends that most likely should be on a credit union's radar. These approximately 15 risk topics provide key questions, answers, and links to related resources.

- Access by entering this URL < www.trustage.com/emerging-risk > within the address bar of your web browser. Access does not require a User ID/Password; however, access to some related resources does require sign-on access to the Business Protection Resource Center.
- Click on the < **Learn more** > to access the risk insights regarding the topic.

Emerging Risks Outlook

Business Protection resources

- [Business Protection Resource Center](#)
- [Business Protection News](#)
- [Emerging Risks Outlook](#)
- [Risk Management overview](#)

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

When risk management is effective, typically nothing bad happens. 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 introduces risks and trends that most likely should be on your radar.

Climate change

Climate change and climate-related risks pose a significant challenge and offer opportunities for credit unions.

[View the white paper](#)

Overdraft / NSF fee litigation for credit unions

Law firms continue to send demand letters threatening a lawsuit and/or file a lawsuit against credit unions alleging members were...

[Learn more](#)

Tips for preventing ransomware incidents and cyber attacks

A ransomware incident is one of the most disruptive and costly attacks your organization can suffer.

[Learn more](#)

Defective post-repossession notices

Class action lawsuits against credit unions due to deficiencies in collection letters continue to be successfully brought forward by...

[Learn more](#)

ATM smash & grab attacks

Criminals are increasingly turning their attention to the money inside automated and interactive teller machines.

[Learn more](#)

Zelle and P2P fraud

Fraudsters continue to target members of credit unions offering P2P (e.g., Zelle) by using a sophisticated scam.

[Learn more](#)


Slips, trips & falls

Surprisingly, slips, trips & fall claims are among the highest in the industry.

[Learn more](#)

Defective post-repossession notices

Class action lawsuits against credit unions due to deficiencies in collection letters continue to be successfully brought forward by plaintiff attorneys.



Class action lawsuits against credit unions due to deficiencies in collection letters continue to be successfully brought forward by plaintiff attorneys. 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. The allegations in these lawsuits involve credit union failures to follow requirements of UCC Article 9 regarding information that needs to be provided in these letters.

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. Some class action lawsuits have resulted in settlements into the millions of dollars.

Ask a risk consultant

Please complete this brief form to route your question to one of our risk consultants.

[Ask a risk consultant](#)

Related resources:

Access TruStage's [Protection Resource Center](#) for exclusive risk and compliance resources to assist with your loss control efforts. The Protection Resource Center requires a User ID and password.

[Collection letters risk overview](#)

On-demand webinar: [Key litigation trends](#) (9/15/2021)

RISK alert: [Class action lawsuits again swirl around collection letter deficiencies](#) (9/1/2020)

Does your credit union use the safe harbor notice of disposition (UCC 9-613/9-614)? +

Are collections staff prohibited from modifying the safe harbor notice? +

Are items listed in the notice of deficiency in the correct order (UCC 9-616)? +

Have you considered other state law requirements (e.g., California)? +

Do you regularly review your collection letters? If relying on an attorney, have you requested and received a written legal opinion that the components of your collection letters are meeting the requirements of UCC Article 9, sections 9-613, 9-614, and 9-616? +

Other Risk Management resources outside of the Resource Center

Credit union employee training

Some specific risks are best mitigated by educating credit union employees on how to respond or interact with specific situations. These credit union employee training web landing pages include access to interactive training modules and additional resources.

The interactive training modules do not require any type of registration so it can easily be accessed by all credit union employees. At the end of each training (approximately 20-30 minutes), employees can print a completion certificate.

Topics currently include:

- Responding to active shooter incidents < www.trustage.com/active-shooter >
- Minimizing common office risks < www.trustage.com/employee-safety >
- When members become victims < www.trustage.com/member-fraud >

Access these pages by < **entering the appropriate URL** > within the address bar of your web browser. Access to the web page or the training module does not require a User ID/Password; however, access to some related resources does require sign-on access to the Business Protection Resource Center.

Click on < **Access training module** > to begin the interactive training.

When members become victims

Each year, fraudsters find new ways to trick people out of money. While some scams involve new approaches, many have been around for decades. Of the over 12.6 million fraud reports, 37% indicated money was lost. In 2023, consumers reported losing nearly \$10.3 billion to fraud according to the Federal Trade Commission¹.

Using common channels like emails, text, phone calls, and even face-to-face interactions, fraudsters typically disguise their identity while retrieving confidential member information. They use tactics to succeed by tugging at the basic human instincts to trust and please. The scams look to catch your members off-guard and to dupe them into making security mistakes or giving away sensitive information and money.

At TruStage™, our goal is to help credit union employees build risk awareness of common scams, understand how to help members with at-question transactions, and share mitigation tips they can use.

Additional resources

- [Common member scams²](#)
- [Protect your identity & money²](#)
- [Don't fall victim: Fraud & Scams eBook²](#)
- [Elder financial abuse risk overview²](#)

Ask a risk consultant

Please complete this brief form to route your question to one of our risk consultants.

[Ask a risk consultant](#)

Access the When Members Become Victims interactive training module

→ Access training module

Access training module

TruStage™

When Members Become Victims

Risk and Compliance Solutions

When Members Become Victims

Start course

TruStage™

MENU

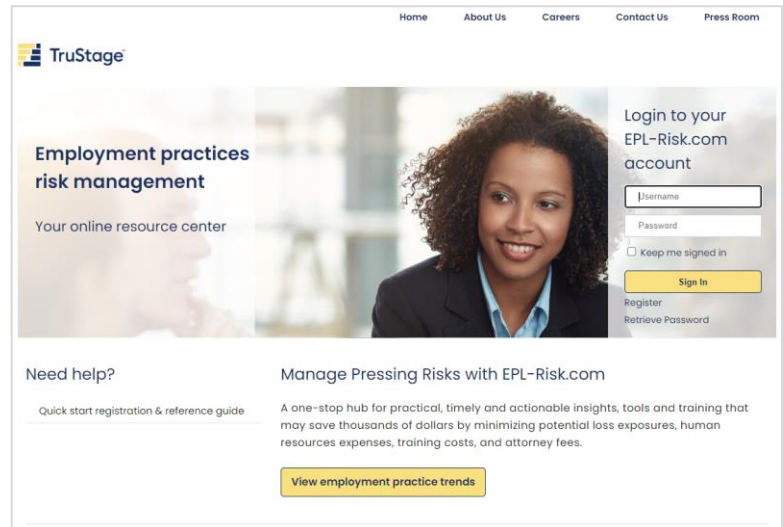
- Introduction
- Start course ✓
- Disclaimer
- How fraud develops
- Recap
- What you will learn
- Common member scams
 - Common fraud scenarios
- Sweepstakes and lottery scams
 - Situational scenario
 - Definition
 - Supporting members
- Elder financial abuse
 - Situational scenario
 - Definition

Partner risk management links

Employment practices risk management resources < www.epl-risk.com >

As a TruStage Employment Practices Liability coverage policyholder, you have exclusive access to easy-to-use risk management tools and resources at www.epl-risk.com. This one-stop resource center provides practical, timely and actionable insights, resources, model policies/procedures, and training to help you and your employees stay on top of current workplace issues, legislation, and employment trends.

A separate User ID and Password is required. Learn more in this [Quick start registration & reference guide](#).

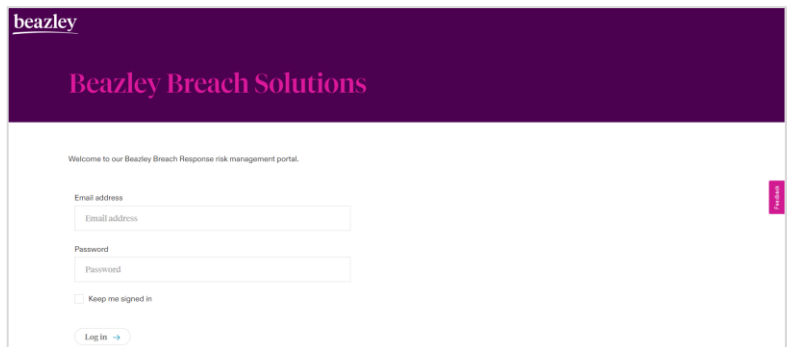


Cybersecurity resources

< www.BezleyBreachSolutions.com >

As a Beazley cyber insurance policyholder, your organization can also access additional cybersecurity resources and training related to compliance & laws, safeguarding information, and preparing to respond to breach incidents.

A separate User ID and Password from Beazley is required. If you need assistance, email bbrservices@beazley.com.

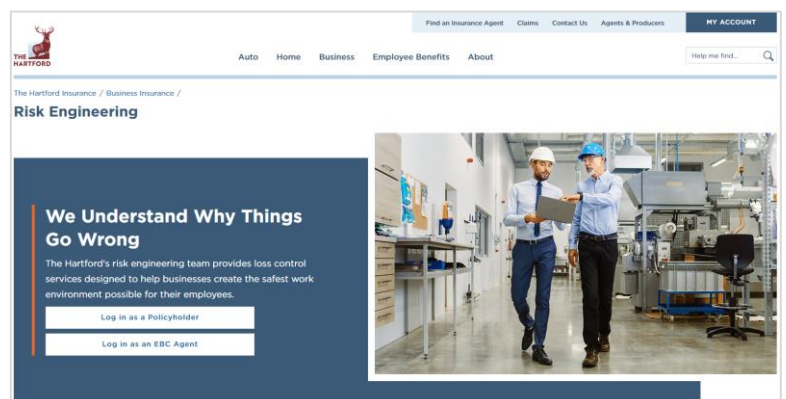


Workplace safety/ wellness resources

< www.thehartford.com/loss-control >

For additional employee safety, wellness, or workers' compensation tools and resources, Workers compensation policyholders of The Hartford provides loss control services and resources to help you create the safest work environment possible for employees.

A separate User ID and Password from The Hartford is required (your policy number is needed). For help with access, contact 800.986.3509 or by emailing RiskEngineering@thehartford.com.





Helping you make confident strategic decisions

Risk & Compliance Solutions

riskconsultant@trustage.com

3,049

Risk consultations/assessments completed

13,583

Total registrants for risk virtual events

97.5%

Virtual event satisfaction score

19,140

RISK Alert subscribers

623,903

Business Protection & EPL Resource Center page views



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

EVP, Chief Retail Officer - \$3.3B credit union

Great webinars - serious, important information delivered in a relaxed, 'we're among friends' way.

Sr. Internal Auditor - \$9B credit union

Really enjoyed the presenters and their real world take on the risks we face currently.

Compliance Specialist - \$51B credit union

Compliance, risk and fraud are constantly changing. Thank you for keeping up and helping us mitigate the risks.

AVP, Compliance - \$914M credit union

Wow! Where do I start? This is one of the best workshops I have attended. Excellent content!

Manager, Internal Audit - \$1.2B credit union



Your risk consultants



Bob Bouvier | Massachusetts

Bob has 30+ years experience specializing in corporate governance, policy development and administrative controls with an emphasis on managing employee dishonesty and fraudulent activity. He graduated from Fitchburg State University and holds multiple designations - CRM, CFE, CCUE, CFSA, CUSFE, and ALICE-certified trainer for active shooter incidents.



Jim Bullard | Georgia

Jim has 10+ years experience in addition to a 23-year banking career in commercial lending and executive risk management. He holds a bachelors in business administration with a specialty in finance from the University of Georgia, in addition to completing the graduate school of banking at Louisiana State University. CUERME & CUBLP designations.



Becky Garton | Wisconsin

17+ years of risk management experience with TruStage. Becky consults with credit unions throughout the country and specializes in the areas of payment transactions, card loss prevention, chargebacks, and compliance. She holds a bachelors degree in elementary education and previously held positions within the payment industry. Becky is also Lean Six Sigma (Yellow Belt) certified which prepares her for project and process improvement work.



Chris R. Gill | Maryland

Chris has 11+ years TruStage experience. He provides the strategic leadership and guidance to the Risk Consultants. He also has multiple years working in the credit union, financial, and risk management sectors. Chris has significant experience in business resiliency, vendor management, internal controls and cybersecurity. He holds a bachelors and masters degree in business administration in addition to having the CUERME designation.



Brad Neumann | Wisconsin

Brad has 34+ years TruStage experience within risk management, business protection, strategic marketing, and training. Previously the Marketing Director at Heartland Credit Union in Madison, Wisconsin, he now provides strategic leadership for TruStage's go-to-market risk and compliance content including the well-known RISK Alert and virtual event programs. He holds a bachelors of science degree in business administration.

Your risk consultants



Ken Otsuka | Illinois

32+ years TruStage experience within risk management specializing in risks associated with payments, deposits, funds transfer/ACH, and fraud. Ken is a commonly-featured as an author for our RISK Alerts and a speaker throughout the U.S. He was previously was an insurance auditor. Ken resides holds a bachelors degree in accounting from Northern Illinois University and is also a Certified Public Accountant (CPA).



Michael Petrone | Maine

37+ years of risk management experience with TruStage. Mike consults with credit unions throughout the country and specializes in the areas of workplace operations, physical security, internal controls, and employee safety. He has multiple designations – CFE, CFSA, and CUSFE – in addition to being an ALICE certified training instructor for active assailant incidents.



Brianda Rojas-Levering | Kentucky

2nd year with TruStage. Brianda brings significant experience helping organizations with legal and regulatory issues including vendor management, contracts, risk, disaster recovery and business continuity, and cybersecurity compliance. Brianda was previously a compliance attorney for a nearly \$2 billion asset-sized credit union. She has a bachelor of arts degree in sociology and juris doctorate of law.



Holly Spiczenski | Wisconsin

30+ year TruStage experience specializing in risks associated with payments/ deposits, including funds transfer and ACH fraud. She spent several years as a fidelity bond claims adjustor; in addition to previously working at a Madison, Wisconsin-area credit union. Holly has a degree in accounting and holds an AIC designation.

Risk management overview

For an overview of Risk Management resources, Alerts, virtual events, and other valued services that TruStage bond policyholders receive, simply go to < www.trustage.com/RMshowcase >. On this page, you can also use an online form to < [Ask a risk consultant](#) > questions regarding a specific risk, related resources, or how to locate resources.

Risk management overview

Actionable insights, relevant resources, and proven risk mitigation guidance help you stay on top of emerging risks within our changing industry.¹

RISK Alerts

Stay up-to-date on the most recent risks facing your industry and stay in-the-know on persistent risks that you need to stay aware of. RISK Alerts are published just-in-time when risks are most prevalent to make sure you are on top of the most relevant topics.

[Text messages & spoofed websites used to lure members into scam](#)

[Vendor impersonation fraud sets up fraudsters to intercept payments](#)

[Credit unions targeted in class action lawsuits related to solar lending](#)

Risk overviews

Risk overviews give you an in-depth look at risk topics you should be aware of for your credit union. Use these overviews to learn what you need to know about specific risks and mitigation tips you should consider.

[Ransomware risk overview](#)

[ATM safeguards risk overview & inspection checklist](#)

[Common member scams](#)

[Responding to an active shooter employee guide](#)

Emerging risk outlook series

Keeping ahead of the complex array of risks, losses, compliance issues, and litigation challenges requires keen awareness, effective preparation, and loss control scrutiny. These emerging risk web pages share critical questions and resources to build awareness and drive credit union action.

[View entire series](#)

Need more help?

With access to actionable insights, relevant resources, and proven risk mitigation guidance through our risk consultants and the Business Protection Resource Center, you can rise above your risk. It is a great way to stay on top of emerging risks within our changing industry.

Questions? Ask a risk consultant

[Access Business Protection Resource Center](#)

Virtual events

Get up-to-the-minute information and proven guidance by taking in a live risk management webinar, office hours, or risk forum. Each session is focused on emerging risks and loss trends impacting credit unions and you gain actionable insights and resources that you can use at your credit union. Most sessions are also available as on-demand recordings.

[View schedule](#)

[Webinar sample: Physical security & technology](#)

Business Protection Resource Center

The Business Protection Resource Center is the central hub for risk management resources including:

- RISK Alert library
- Loss prevention library
- On-demand training & education
- Access to additional partner resources related to cybersecurity, employment practices, and workplace safety/wellness

You can also easily report a risk/scam or even schedule a 1:1 discussion with a risk consultant.

[Visit the Business Protection Resource Center](#)

Experienced risk consultant team

By analyzing exclusive insights, experienced risk consultants proactively support your risk management efforts by sharing guidance and best practices through resources and 1:1 consultations.

[Meet your team](#)

[View risk management overview](#)

[Risk management resource snapshots](#)

Additional insights?

If you'd like to discuss this risk in more detail, simply schedule a no-cost 1:1 discussion with a TruStage™ Risk Consultant by contacting us at riskconsultant@trustage.com or 800.637.2676.

This resource is for informational purposes only. It does not constitute legal advice. Please consult your legal advisors regarding this or any other legal issues relating to your credit union. TruStage™ is the marketing name for TruStage Financial Group, Inc., its subsidiaries and affiliates. TruStage Insurance Products offered to financial institutions and their affiliates are underwritten by CUMIS Insurance Society, Inc. or CUMIS Specialty Insurance Company. Cyber policies are underwritten by Beazley Insurance Group or other nonaffiliated admitted carriers.

This summary is not a contract and no coverage is provided by this publication, nor does it replace any provisions of any insurance policy. Please read the actual policy for specific coverage, terms, conditions, and exclusions.

10011470-0724 © TruStage