TruStage™

Don't fall victim

Fraud & scams eBook

Each year, fraudsters find new ways to trick people and financial institutions out of money.

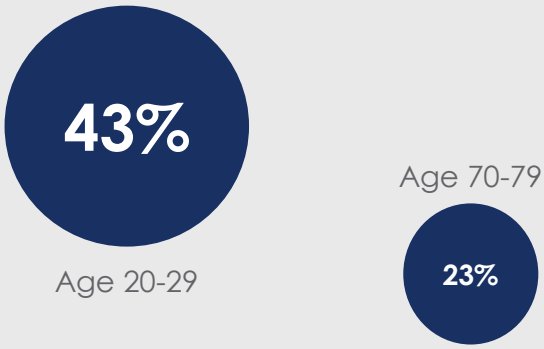
While some scams involve new tricks, many have been around for decades. Of the nearly 2.4 million fraud reports, 26% indicated money was lost. In 2022, consumers reported losing more than $8.8 billion to fraud according to the Federal Trade Commission.

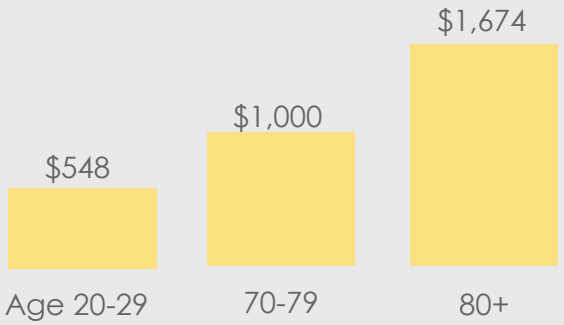
Fraudsters target the weakest link: humans
Using common channels like emails, text, and phone calls; fraudsters typically disguise their identity while retrieving confidential member information. They use tactics to succeed by tugging at the basic human instincts to trust and please. The scams look to 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.

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.

Younger people lost money to fraud **more often than older people**





But when people aged 70+ had a loss, **the median loss was much higher**

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

P2P/Zelle fraud

Fraudsters continue to target members of credit unions offering Peer-to-peer payments (e.g., Zelle) by using a sophisticated scam to defeat two-step authentication which leverages the use of one-time passcodes.

The Zelle/P2P fraud scam is widespread and continues to grow as the social engineering tactics continue to evolve.

The traditional Zelle/P2P fraud scam surfaced in 2019 and starts with fraudsters sending texts to members appearing to come from the credit union warning members of suspicious transactions on their accounts.

The fraudsters call the members who respond to the texts - spoofing the credit union's phone number - and claim to be from the credit union's fraud department. The fraudster tells the member they are calling to discuss the suspicious transactions but must first verify the member's identity and ask for the member's online banking username. The fraudster then tells the member that he or she will receive a passcode and the member must provide it over the phone to the fraudster.

The fraudster initiates a transaction, such as the forgot password feature, that triggers the passcode to the member. Upon receiving the passcode from the member, the fraudster uses it to reset the member's online banking password, allowing the fraudster to login to the member's account, and use Zelle / P2P to transfer funds.

Zelle Yourself has fraudsters conning members into transferring funds via Zelle to themselves using the members' own mobile phone number under the guise that it will replace funds stolen from their account; however, the fraudsters receive the transfers.

- Fraudsters sends text alert to members - appearing to come from the credit union - asking the members if they attempted a large dollar Zelle transfer.
- Fraudsters immediately call those members – spoofing the credit union's phone number – who respond 'NO' and claim to be from the credit union's fraud department.
- Fraudsters tell the members the Zelle transfers went through, but the funds can be recovered.
- Fraudsters tell the members in order to recover the stolen funds they must use Zelle to transfer the funds to themselves using their own mobile phone number.

  Note: The fraudsters previously established their own Zelle account and may have opened an account at the credit union to do so. Members are conned into disabling their mobile phone number associated with their Zelle account. The fraudsters link the members' mobile phone numbers to the fraudsters Zelle accounts.
- The transfers actually go to the fraudsters.

Mail theft/check fraud

Mail theft and armed robberies against U.S. Postal Service carriers has increased substantially throughout the country. The criminal's focus is to gain access to the master keys of the blue USPS mailboxes – ultimately in search for checks that can be altered, counterfeited, or sold online.

There has been a significant increase in losses involving fraudulent checks drawn on member accounts. This increase is due in large part to the stolen mail problem in several states. Fraudsters are stealing members' issued checks and manufacturing fraudulent checks using information from the stolen checks.

In several cases, member-issued checks have been stolen from USPS mailboxes, as well as from members' mailboxes.

After stealing checks, fraudsters:

- Alter the payee and dollar amount.
- Manufacture fraudulent checks.
- Use the checks to open fraudulent new accounts and/or apply for loans using the accountholder identities listed on the checks (e.g., name and address information).

Credit union recourse

Credit unions have recourse against the depositary institutions that accept altered checks under UCC 4-208, Presentment Warranties. Credit unions can recover the loss by pursuing a breach of presentment warranty claim against the depositary institutions that accepted the altered checks.

Refer to Liability for forged endorsements and alterations risk overview for guidance and a sample letter to use to pursue a breach of presentment warranty claim against depositary institutions

Encourage members

- Pay bills online or use the credit union's bill paying service.
- Mail checks inside the Post Office lobby rather than using blue mailboxes.
- Log into credit union accounts frequently to review their transaction history – looking for unfamiliar transactions.
- Report unfamiliar and unauthorized transactions immediately to the credit union.

Business email compromise

The fraudster's intent is to catch an employee off-guard and induce them to act quickly to make a wire transfer, payment, or transfer sensitive data to cybercriminals. These urgent requests often exceed $1 million. According to the FBI, $2.7 billion adjusted loss for BEC crimes occurred against businesses & consumers in 2022 (IC3's 2022 Internet Crime Report).

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 virtual meeting scams using deepfakes or digitally-altered recordings. The surge of business email compromise (BEC) and fraudulent instruction scams typically request large wire transfers.

BEC scams typically involve an executive level employee's email or phone number that has been compromised or spoofed through a phishing attack. The fraudsters create an email or text appearing to be sent from the executive to another individual within the organization requesting a payment – typically wire transfer, purchase of gift cards – divert payroll, or request employee W-2 information.

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

From: CEO@acmecorp.com
To: Jane@acmecorp.com
SUBJECT: Urgent

I need you to initiate a wire transfer in the sum of $45,250 to the account below. I am boarding a flight and this needs to be done right now. Can you please get this done? Send confirmation of the transfer immediately only to this email.

Thanks

Sample email with highlighted warning signs

Warning signs

- The request encourages the recipient to think and act fast with a sense of urgency.
- Requests typically come from a high-level executive or authority.
- Requests often coincide with being out-of-the-office as they've accessed calendars.
- The request asks the recipient to keep transaction confidential and only communicate through email.
- Requests often coincide with changes in direct deposit information or for payments to be made to a different account.
- The request may impersonate a trusted supplier, vendor or business partner to advance the fraudster's schemes.
- Look for common red flags that are associated with any compromised email, such as misspellings, poor grammar, a sense of urgency, and emails sent outside of normal business hours.

Fraudulent instruction

Like business email compromise, fraudulent instruction wire scams involve a fraudster looking to trick a member, credit union employee, or even a title company or closing agent. The scam is usually conducted via email with fraudulent instructions to wire funds to the fraudster at the last minute.

How the real estate fraudulent wire scam works

- A fraudster hacks into a title company or lender's email server or computer system to search for upcoming real estate closings.
- Shortly before 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."
- Common email subject lines are: "Our Wiring Instructions Have Been Updated" or "We Have Sent You the Wrong Wiring 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!

Member loss: $187,000	Credit union loss: $1.7 Million
• Member buying a new house with sufficient funds on deposit at credit union • Title company's email was hacked – fraudster found loan closing information • Fraudster sent a spoofed email to member with "updated wire instructions" • Member requested the wire in person at a branch	• Credit union mortgage department employee's work email hacked • Fraudster found email exchanges with title company president • Fraudster spoofed title company president's email and sent email to employee with "updated wire instructions" for all future closings • Impacted 3 members' closings

Source: Internal Claims Data, TruStage, CUMIS Insurance Society, Inc.

Mitigation tips

- Establish procedures to call the title company/closing agent using a reliable phone number to verify the legitimacy of wire instructions received by email or fax;
- Implement the use of a passcode with the title company/closing agent in advance to be used in conjunction with your callback and verification process;
- Require the title companies/closing agents to use encrypted emails when sending wire instructions;
- If your member received the wire transfer instructions by email, verify the instructions and information with the title company/closing agent separately prior to sending the funds on the member's behalf;
- Look for common red flags that are associated with any compromised email, such as misspellings, poor grammar, a sense of urgency, and emails sent outside of normal business hours;
- Be suspicious of emails that contain last minute changes in payment type or account numbers; and
- Educate your members about the possibility of this scam and how to protect themselves. Remember, the member could be liable for the loss of their funds, if the fraud was perpetrated against the member.

Account fraud

Fake consumers, or synthetic identities, obtain countless deposit accounts, credit card accounts, auto loans, and personal loans costing credit unions each year.

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

Account takeovers
Two common approaches that fraudsters use:

- 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).

New account fraud
New account fraud losses are increasing through the online channel. Fraudsters who open accounts 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 credit union call center and often request changes to members' contact information (e.g., phone number, email address, etc.). This typically leads to other forms of fraud, such as requesting wire transfers through the call center.

Many think of a fraudster as a shady character working alone in a dark room. Yet, fraudulent activities are often generated by individuals trained to develop emotional and personal connections to manipulate others.

Typical fraudster approach

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

Fraudster's 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

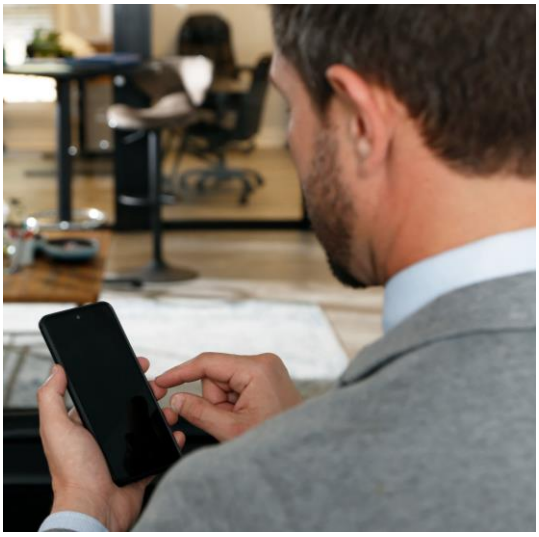
Fraudsters tend to gravitate to the phone channel because the primary line of defense — call center representatives asking challenge questions — is highly vulnerable to social engineering.

Social engineering fraud

27 million American consumers are reportedly victimized by identity fraud-related financial losses.

Source: Javelin 2022 Identity Fraud Study "The Virtual Battleground"

Social engineering fraud is range of malicious activities carried out by fraudsters through human interactions. It uses psychological manipulation to trick users into making security mistakes. Unsolicited emails, text messages, and telephone calls purportedly from a legitimate company or individual requesting personal, financial and/or login credentials are common approaches.



- **Phishing** - One of the most popular forms of social engineering attempts to acquire sensitive information such as usernames, passwords and account or card details by masquerading as a trusted entity and creating a sense of urgency, curiosity or fear in victims. It then prods recipients into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.
- **SMiShing** - A type of phishing attack where cell phone users receive text messages containing a website or document hyperlink; which, if clicked would lead to a malicious URL and/or download malware to the cell phone. It could appear to come from the recipient's credit union with an intent to gain their personal or account information. In addition, there could be a request to call a fraudulent phone number.
- **Vishing** - Voice phishing is the telephone equivalent of phishing attempting to scam the user into surrendering private information that will be used in identity theft. Often, the call will come from a spoofed phone number making it look like the credit union is calling the member which will provide the member with a sense of legitimacy.

The call center is often a first stop for fraudsters.
Call centers are often considered key "soft" targets to deliver sensitive member details. Regardless of the fraud type or intention, the scammers' first objective is to convince a call center representative that they are a real member.

Fraudsters gravitate to the phone channel because the primary line of defense — call center representatives asking challenge questions — is highly vulnerable to social engineering. It is easier for fraudsters to find answers to challenge questions and then social engineer a rep into granting access to a member account than it is to hack IT infrastructure backed by a dedicated security team.

Common consumer scams

Romance scams

Using fake online dating profiles with photos of other people, scammers say they are from the U.S. but are temporarily traveling or working overseas. Most romance scams start with fake profiles on online dating sites created by stealing photos and text from real accounts or elsewhere. Some of the fictitious occupations include working on an oil rig, in the military, or as a doctor with an international organization.

Scammers quickly profess their love and tug at the victim's emotions with fake stories and their need for money. They often request money for reasons such as a plane ticket, other travel expenses, and customs fees – all needed to get back into the country. The victims often wire their "sweetheart" scammers money or share login credentials.

Tech support scams

Someone calls and says they're a computer technician. They might say they're from a well-known company like Microsoft or Apple, or maybe your internet service provider. They tell you there are viruses or malware on your computer, and you'll have to provide remote access to your computer or buy new software to fix it. These scammers might want to sell you useless services, steal your credit card number, or get access to your computer to install malware, which could then let them see everything.

Advanced fee scams

In the advanced fee scam, the scammer informs a victim that he/she has won a large award (think bogus lottery scam) or is entitled to a large inheritance from a deceased relative. However, before the victim can receive the money, he/she must supposedly pay taxes or fees. The victim ends up wiring funds to the scammer to pay the taxes or fees but never hears from the scammer again.

Social Security, Government & IRS scams

Scammers impersonating Social Security Administration employees over the phone to request personal information or money. Imposters may threaten consumers and demand immediate payment to avoid arrest or legal action. Many calls "spoof" official government numbers, such as SSA's National 800 Number, the Social Security Fraud Hotline, local Social Security field offices, or local police numbers. In addition, impostors may use legit names/phone numbers.

Similarly, calls from someone who says they're from the IRS. The caller may know the SSN. They say back taxes are owed, or involved in money laundering, drugs, etc. They threaten to lawsuit, arrest / deport, or revoke the SSN or license if payment is not made immediately. In order to avoid legal action, they ask for account info or are asked to send money in the form of gift cards, wire transfer or cash.

Secret shopper scams

Members looking to earn extra cash are frequently tricked into participating in the secret shopper scam. If a member accepts the job, he/she receives a counterfeit cashier's check ranging from $2,000 to $5,000. They are instructed to cash the check and purchase money orders and gift cards and send them to the scammers. For their efforts they will keep a percentage of the check they receive. The counterfeit check is subsequently returned unpaid and charged back to the member's account.

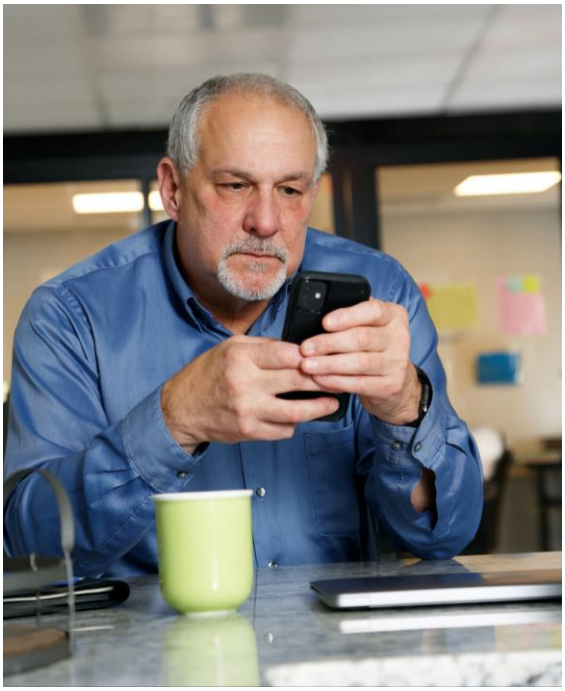
Relief scams

Scammers attempt to take advantage of times of uncertainty to con people into giving up their money to aid those in need in fraudulent relief funds. Recent scams that have been attempted: flood / disaster relief; Covid-19; Ukrainian assistance; student loan debt forgiveness; and other charity scams.

Common consumer scams

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.

Encourage employees and members to follow these tips:



- Don't always trust the name - criminals will spoof the email name to appear to be a legitimate sender
- Check for misspelled words, bad grammar, and/or typos
- Be cautious of clicking links and opening attachments – Don't click unless you are confident of the sender or are expecting the attachment
- Do not provide personal or account information when asked. Openly sharing information on social media can provide the necessary information to impersonate you or answer some challenge questions.
- Do not share a one-time passcode sent via text or email to your device(s)
- Check email salutations - many legitimate businesses will use a personal salutation
- Be suspicious of "urgent" or "immediate" response needed or "unauthorized login attempt" of your account
- Know the IRS or Social Security Administration will not contact you by phone, email, text or social media
- Don't believe everything you see. Brand logos, names and addresses may appear legitimate
- Be suspicious of random or unusual groups of people (e.g., all last names begin with same letter) on the to/recipient list
- Watch for emails or texts that appear to be a reply to a message that you didn't actually send
- Monitor the sender's email address for suspicious URLs & domains – using similar letters and numbers
- If something seems suspicious; contact that source with a new email or phone call, rather than just responding or replying directly to the email, text, or call
- Be wary of offers that appear too good to be true, require fast action, or instill a sense of fear
- Keep social media accounts private and be cautious who you're connecting with
- Never share anything related to your credit union account, transactional history, or identifying information in an unprotected public forum

Elder abuse & exploitation

Elder abuse in the form of financial exploitation is at an all-time high and will continue to grow as this population category continues to grow daily. The number of elderly fraud victims has risen at an alarming rate, while the loss amounts are even more staggering.

Elderly member scam
An elderly member receives a call from someone pretending to be their grandchild (the perpetrator may or may not know the grandchild's name). The "grandchild" indicates they have been arrested, and they need money to make bond. Circumstances, may vary or be embellished such as they have unpaid tickets they must pay before being released, or they are calling the grandparent because they don't want their parents to know.

The "grandchild" requests an amount of money needed and provides wire instructions which includes an account number of where to send the funds. The grandparent contacts the credit union and requests the wire transfer. The funds are then wired to an account controlled by the fraudster.

Contact center scam
A fraudster calls the credit union pretending to be an elderly member with a request for a new debit card since they lost the previous card. The fraudster looks to defeat weak authentication based upon known key information that a relative or someone with a legitimate purpose for being in the victim's house (e.g., caretaker) might be aware of. By defeating authentication over the phone, the scam continues and the "replacement card" is sent to the address on file where it is captured and used to gain access to account funds.

Older members that begin using services such as debit cards, home banking, wire transfers and P2P transactions - which have not previously - are common red flags.

Face-to-face exploitation
An elderly member walks into the credit union with an individual they introduce as a relative or as a friend. They indicate they would like to add this person to their account as a joint owner, including being authorized to access their safe deposit box. The individual could be a legitimate relative, or someone the victim knows, since in many cases the exploitation is perpetrated by an individual known to the victim.

Once the fraudster is added to the account, they can access account funds in various transactions (e.g., wires, withdrawals, P2P). Additionally, by gaining safe deposit box access, individuals can get cash, jewelry, wills, and other important documents. In some instances, older adults have lost their complete nest egg.

Source: 2022 FBI Elder Fraud Report, IC3

Ransomware

Ransomware-related data breaches have **doubled in each of the past two years**. At the current growth rate, ransomware attacks will pass phishing as the number one root cause of data compromises in 2022.

Source: 2022 ITRC Annual Data Breach Report, IDTheftCenter.org

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

Unfortunately, it's getting easier to deploy ransomware and malware, and that gives threat actors more access than ever before. Tools – such as do it yourself Ransomware-as-a-Service (RaaS) kits - are cheap to obtain and competition between ransomware providers has driven entry costs down. In addition, some tools are publicly available and anyone with minimal coding skills can re-use them.

There is also evidence that threat actors do not always honor their word to destroy exfiltrated data if the ransom is paid. Even if the original threat actor has been paid, it remains nearly impossible to ensure that the information is not accidentally or intentionally shared with other threat actors. This is one reason why fewer victims are paying a ransom.

Threat actors are typically indifferent to which type of organization pays them as long as they are getting paid. This is being done to try and justify larger initial demands in the hopes that they result in large ransom payments.

- Unfortunately, six- and seven-figure demands have become routine among ransomware attacks.
- While the most identified infection points remain phishing emails, corrupt attachments, and weak remote desktop protocols (RDP); unpatched systems, extensive reuse of passwords - a lack of multi-factor authentication has also contributed to the increase in successful entry.
- Ransomware operators are placing more effort towards remaining undetected on a breached network - commonly referred to as dwell time. Increased dwell time provides opportunities to escalate hijacked privileges while searching for data caches of sensitive information that can be exploited.

24 days
average downtime

$409K
average ransom payment

Source: Coveware Quarterly Ransomware Report – January 2023

Don't fall victim

Knowledge gives you power to take action

Fraudsters attempt to target the weakest link: humans. They use tactics to succeed by tugging at the basic human instincts to trust and please. And 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.

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.

Keeping ahead of the complex array of ever-changing risks, loss trends, and fraud/scams that are impacting credit unions and your members requires keen awareness, effective preparation, and loss control scrutiny. While each credit union has its own unique risk footprint, be sure to:

Provide employees, volunteers, and members with fraud/scam education and knowledge along with proactive tips to ensure personal and sensitive information is not compromised.

Encourage employees and members alike to be suspicious of unsolicited emails, texts, and phone calls

Look to recognize the psychological fraudsters often use such as power, authority, enticement, speed and pressure.

Looking for additional insights?

- Access the **Business Protection Resource Center** (User ID & password required) for exclusive risk and compliance resources to assist with your loss control efforts.
- Go to **Emerging Risks Outlook** for critical questions, answers, and resources to help build additional awareness and drive organizational action.
- 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 at **800.637.2676**.

10009839-1023 © TruStage

TruStage™