



Risk & Compliance Solutions | Risk Overview

Fraud trends

Navigating the deposit and payment landscape

Proprietary and confidential. Do not distribute.



Don't fall victim



Each year, crafty fraudsters find different ways – email, text, phone, and even in-person - to trick consumers and financial institutions.

→ Of the **2.6 million fraud reports**, 38% of consumers indicated money was lost for a **total of \$12.8 billion**.

Source: Consumer Sentinel Network Data Book 2024, Federal Trade Commission



Fraud trends on the radar



Account takeovers



ITM fraud



Jackpotting



Check fraud & kiting



Card fraud



Wire fraud

Fraudsters look to catch you off-guard and/or to dupe you into making security mistakes or giving away sensitive information and money.

Fraud trends on the radar

Account takeovers



Account takeovers



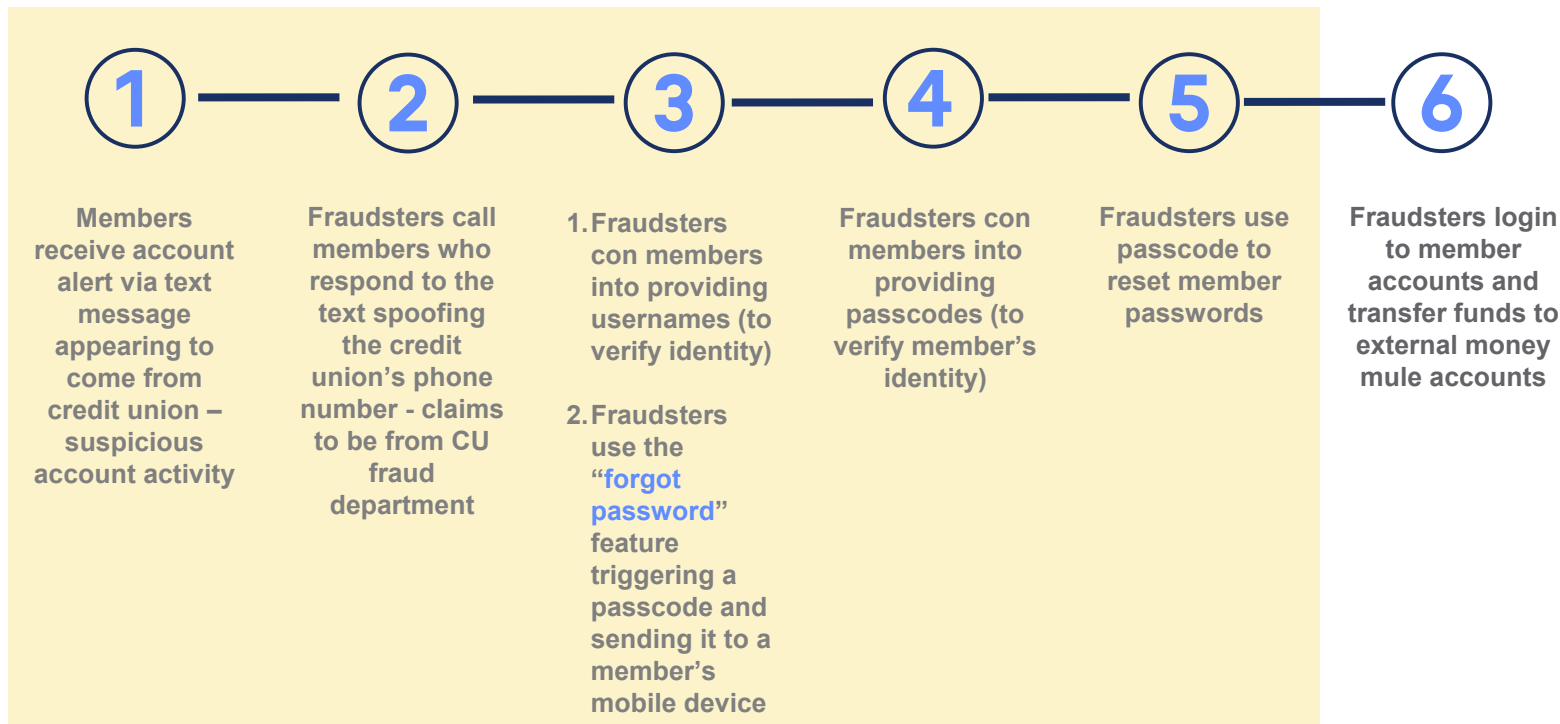
- **Leading source** of loss across the industry
- Incidents are growing in scale and complexity
- Recent losses have involved hundreds and thousands of compromised accounts, amplifying the overall financial impact
- Multiple seven-figure account takeover fraud losses reported

Primary risk drivers

- Typically driven by social engineering campaigns targeting members, where fraudsters trick individuals into revealing credentials, authentication codes, or other sensitive information
- Once access is obtained, fraudsters quickly extract funds using multiple channels, including wires, ACH transfers, peer-to-peer payments, and ATM withdrawals
- Also, target contact center employees to reset member passwords and change member contact information
- Enroll member accounts for online banking
- Fraudsters are increasingly pivoting to alternative methods, demonstrating a high level of adaptability

Account takeovers

Deploy tactics from Zelle fraud scheme



Another variation of the scheme has fraudsters skip sending fraudulent text alerts and proceed directly to calling members spoofing the credit union's phone number to con them out of their login credentials.

Variation of scheme

- Text messages contain a link to spoofed website – CU online banking login
- Members click on the link and enter login credentials
- Fraudsters used credentials to immediately login to member accounts
- 2-factor authentication passcode delivered to members
- Members entered passcode to the spoofed site
- Fraudsters grab passcodes to complete login to member accounts
- Fraudsters transfer funds to external money mule accounts

Account takeover

\$2M fraud loss

- Members received a text alert appearing to come from the credit union – suspicious debit card transactions
- Members responding to the text received an immediate call from the fraudsters spoofing the credit union's phone number
- Fraudsters claimed to be from the credit union
- Fraudsters conned members into providing their online banking usernames – to verify their identities
- Fraudsters used the usernames with the “**forgot password**” feature – triggering a 2-factor authentication passcode to members
- Members conned into providing the passcode to the fraudsters – to verify their identities
- Fraudsters used the passcodes to reset members' passwords
- Logged into accounts and used A2A/external transfer service to transfer funds to external money mule accounts - \$2M in transfers in < 2 weeks
- Disabled A2A/external transfer service and fraud stopped

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

Digital Banking

Manage your accounts and cards, transfer money, and track your financial wellness.

User ID:

Password:

[Register](#)

Log in

[Forgot Password?](#)

[Forgot User ID?](#)

Trending!

Account takeovers & money mules



Money mule

Risk overview



Money mules are recruited by fraudsters to assist in laundering money obtained through illicit activities, such as money stolen from victims of fraud. In many cases, fraudsters recruit money mules with bogus job offerings through online job ads or social media with promises to earn easy money for minimal work. Money mules add layers of recipients to the money trail which complicates law enforcement's ability to track the money from the victims to the fraudsters.

Types of money mules

Typically, money mules fall within three categories:

- **Unwitting participants**
These money mules are typically recruited through online job scams, won a sweepstakes, or strike up an online relationship and are unaware that they are engaged in criminal activity.
- **Witting participants**
These money mules are aware that they may be involved in suspicious activity but engage in it anyway.
- **Complicit participants**
These money mules are fully aware that they are engaged in criminal activity.

Money mules may open accounts under their own identity. Alternately, they may be instructed to open the accounts using a stolen or synthetic identity.

Money mules may be instructed to open an account, including business accounts, at a specific financial institution or use their own account to receive the funds. Fraudsters transfer funds from accounts of fraud victims to the money mule accounts. Upon receipt, the money mules are typically instructed to wire the funds elsewhere. Alternately, the money mules may be instructed to purchase cashier's checks, convert the money to virtual currency, purchase gift cards, or a combination of these actions.

Money mules are also recruited to cash stolen checks, such as U.S. Treasury checks. The money mules are instructed to open accounts, including business accounts, at financial institutions in the name of the payees listed on the checks to deposit the stolen checks and transfer the funds elsewhere.

Typical money sources

- Account takeovers
- Wire fraud, including business email compromise and related scams, such as vendor impersonation
- Online romance, job, or sweepstakes scam victims
- Other credit-push payment scams

Upon receipt of the funds, the money mules are instructed to transfer the funds elsewhere. The transfers may be to other money mules in the network or to accounts controlled by the fraudsters. The transfers may be by wire or ACH using external transfer service.

Money mule solicitations are commonly disguised as work from home opportunities, usually to process payments.

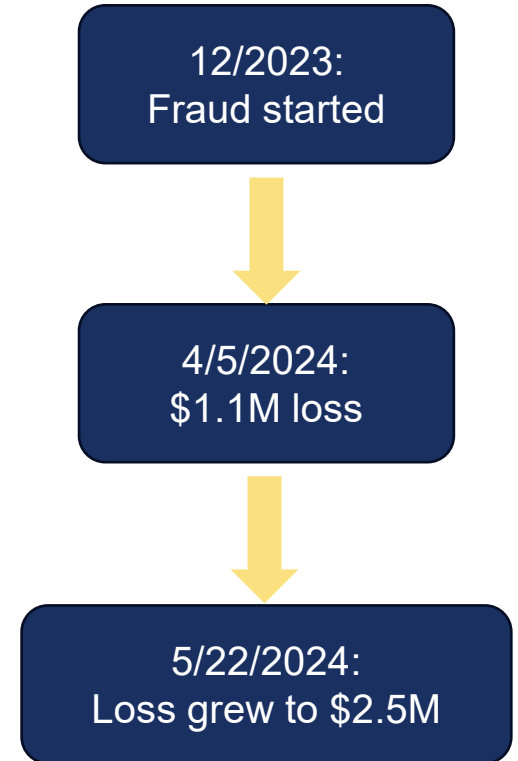
Account takeovers & money mule accounts at the same credit union

- Fraudsters recruit money mules to open fraudulent accounts at target credit union
- Social engineering attack launched against existing members to con them into providing their login credentials once the mule accounts are opened
- Fraudsters use member-to-member (M2M) transfer feature to make large dollar transfers from compromised member accounts to the money mule accounts
- Money mules withdraw funds through various means

Account takeover

\$2.5M fraud loss

- Fraudsters recruited money mules to open accounts at the credit union
- Fraudsters called existing members spoofing credit union's phone number claiming to be from credit union's fraud team
- Conned members into providing usernames that fraudsters used with the "forgot password" feature
 - Triggered 2FA passcodes to members – provided to fraudsters
 - Fraudsters used passcodes to reset passwords
- Fraudsters initiated large dollar M2M transfers to the mule accounts
- Money mules initially withdrew the funds in-person at branches but pivoted to electronic withdrawals



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

Account takeovers & Reg E protection

Reg E's definition of an unauthorized EFT [§1005.2(m)]

“Unauthorized electronic fund transfer” means 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.

Additional clarification in the commentary to §1005.2(m)

3. Access device obtained through robbery or fraud. An unauthorized EFT includes a transfer initiated by a person **who obtained the access device from the consumer through fraud or robbery.**

CFPB's EFT FAQs

The CFPB's Electronic Fund Transfers FAQs clearly indicate that members victimized in this con are entitled to Reg E protection and should be recredited.

Members victimized in this con are entitled to Reg E protection.

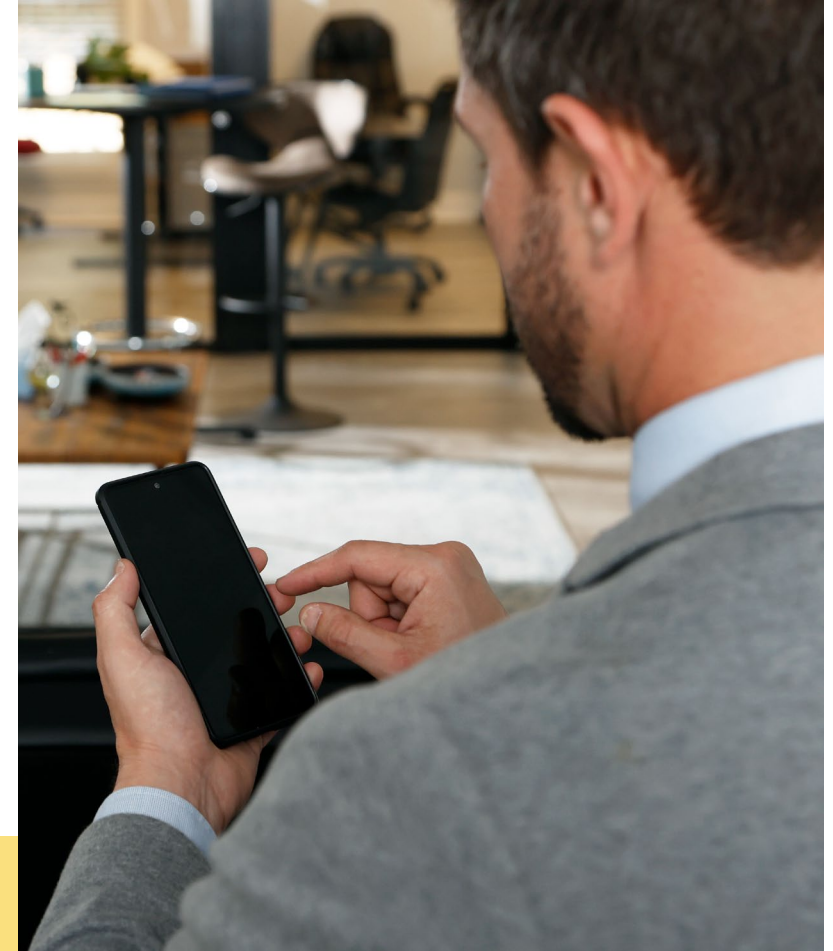
Refer to the CFPB's Electronic Fund Transfers FAQs:
<https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/>

Account takeover

\$800k online wire fraud loss

- Credit union offered online wires through online banking (consumer platform)
- Online wire requests processed by a credit union employee
- Fraudster impersonated a member and social engineered call center employees
 - Reset member's online banking password
 - Changed member's contact information (home & mobile phone numbers; email address)
- Fraudster logged into account
 - 2FA triggered but passcode delivered to fraudster via text message
 - Requested 2 wires totaling \$800k
- Callback verifications were performed but calls went to the fraudster who answered security questions

Note: Wire transfers are governed by Article 4A of the Uniform Commercial Code (UCC 4A)



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



Account takeover risk mitigation

- Deploy strong online banking layered security controls
 - A more secure form of 2-factor authentication – such as a token or push notifications to a dedicated app on members' device
 - A real-time fraud monitoring solution with behavioral analytics that leverages AI and machine learning
- Don't allow members to use the "forgot password" feature using an unregistered device
- Set reasonable monetary limits, including external transfers, P2P, bill pay, M2M transfers and wires
- Avoid resetting passwords based on a member's phone request
- Properly authenticate members enrolling for online banking through credit union's website – avoid sending online banking enrollment passcodes via email due to email hacking risk

Important fraud rules

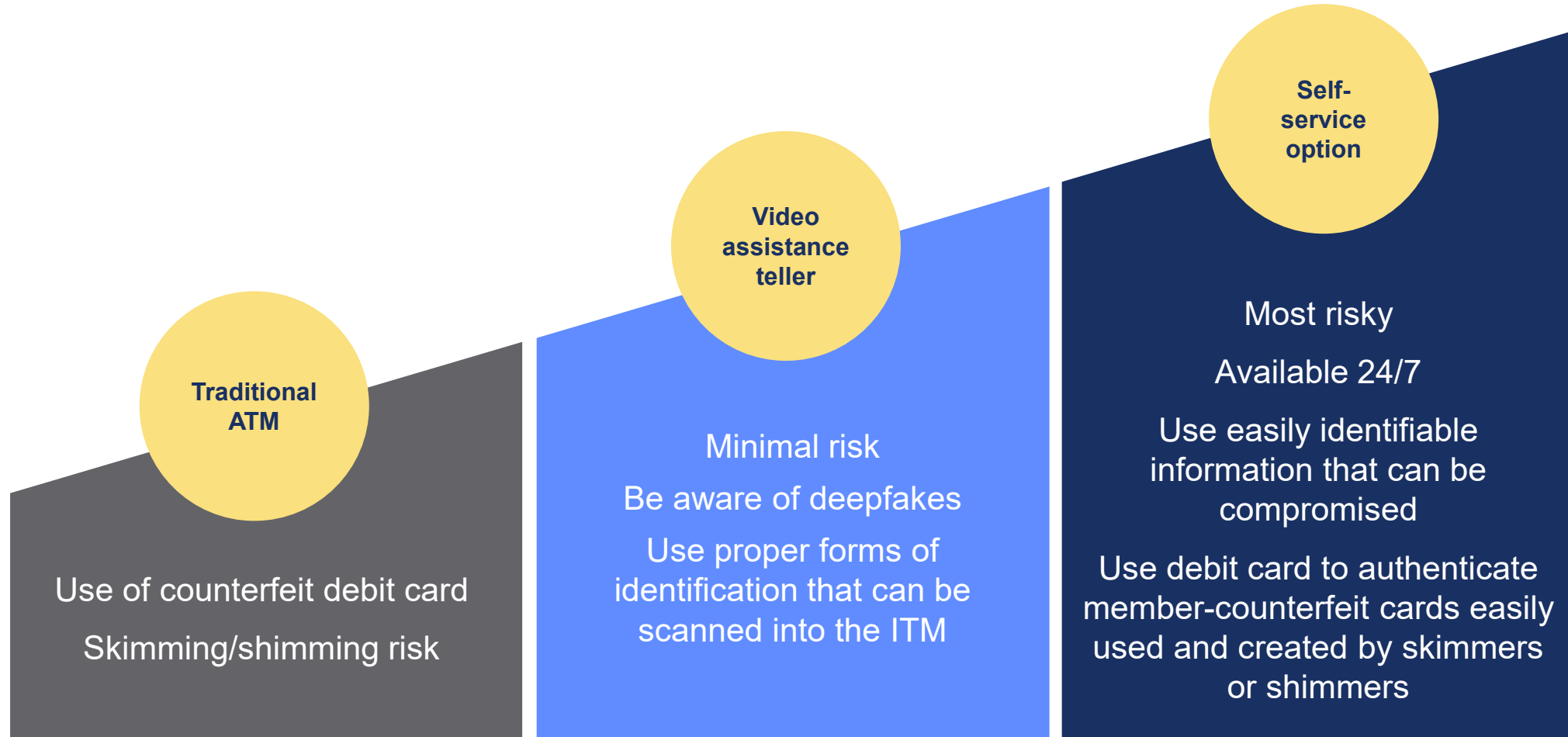
- Block/review external transfers, M2M transfers, bill pay, wires, and P2P transfers that are initiated immediately following a password reset
- Block/review large-dollar M2M transfers to new accounts OR create rule to prevent M2M transfers to new accounts for the first 30-60 days of account opening

Fraud trends on the radar

ITM fraud



ITM fraud risks



ITM fraud – unauthorized withdrawals from member accounts

What's happening?

- Fraudsters target the ITM's self-service feature at outside ITMs during non-business hours (late night over weekends)
- Access member accounts using counterfeit debit cards at ITMs
- Many credit unions found deep insert skimmers on their machines
- Others had fraudsters access member accounts using an alternate authentication allowed by the ITM – such as a combination of account number plus SSN or date of birth
- In some cases, fraudsters took advances against member home-equity line-of-credit (HELOC) loans at the ITMs
- Mid six- and seven-figure losses are common



ITM fraud risk mitigation

In general:

- Block all fallback transactions at ITMs and ATMs
- Set reasonable daily withdrawal limits
- Use skimming/shimming detection technology
- Conduct daily inspections of all ITMs/ATMs – including opening to inspect for deep shimmers
 - If foreign device or tampering is detected – machine should automatically shut down
- Ensure all ITMs and ATMs are EMV-enabled
- Educate members of risk at ITM/ATMs – report any signs of tampering

ITM self-service option:

- If a debit card is used to authenticate members, ensure ITM reads the EMV chip, if it is not detected decline the transaction
 - Do not allow fallback transactions
- Avoid using easily compromised identification to access accounts (i.e.: SSN, DOB, account number)
 - Implement one-time passcodes sent to member devices before proceeding with transaction access
- Set reasonable daily withdrawal limits
 - Single transaction and daily limits
- Do not allow access to line of credit accounts
- Limit hours of operations to normal business hours for self-service option and require members to use video teller if available. Machines can function as ATM during nonbusiness hours

ITM fraud case studies

Credit union A

- **Date of loss:** March 24, 2023
- **Members affected:** 197
- **Total loss:** \$1,747,785
- **Loss per member:** \$8,872
- Withdrawals occurred over a 4-hour period using the self-service feature
- Multiple individual member losses over \$50,000

Credit union B

- **Date of loss:** March 4, 2024
- **Members affected:** 302
- **Total loss:** \$393,990
- **Loss per member:** \$1,305
- Withdrawals occurred over a 6-hour period using the self-service feature



The disparity in losses:

- Both credit unions had a single withdrawal limit of \$2,500 but Credit Union A did not have a daily limit – fraudsters made multiple \$2,500 withdrawals from a single member's account
- Credit Union A allowed members to take advances against line-of-credit loans (e.g., HELOCs) using the self-service feature while Credit Union B did not
- Credit Union A: Fraudsters took advances against member HELOCs to fund the withdrawals

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

Fraud trends on the radar

Jackpotting – ATM/ITM



ATM/ITM jackpotting – causes machine to dispense cash

- **Man-in-the-middle attack.** Fraudsters install a device between the machine's computer and the network cable connection to the acquirer's host system. Requires the fraudsters to insert any card - like a gift card or a stolen card – and messages are intercepted and modified
- Fraudster **infects the machine with malware.** Usually by inserting a flash drive containing malware into the USB port – simply by accessing the ATM/ITM top hat
- Fraudsters connect a **black box**, usually a laptop, directly to the ATM dispenser to send commands to the machine to disburse cash until its empty





Jackpotting mitigation tips

- Work with ATM/ITM vendor
- Replace the ATM/ITM top hat lock and equipping it with an alarm is critical - use an audible alarm to startle the criminal and get them to flee
- Encrypt the machine's hard drive
- Encrypt the communication between the machine and the acquirer's host system. If a router is used, the communication link between the machine and the router must also be protected.
- Ensure the ATM/ITM operating system is supported
- Always ensure security patches are installed when they're made available
- Send a technician to any ATM/ITM that has been offline for at least 5 minutes
- Conduct daily machine inspections

Fraud trends on the radar

Check fraud, fraudulent deposits & kiting



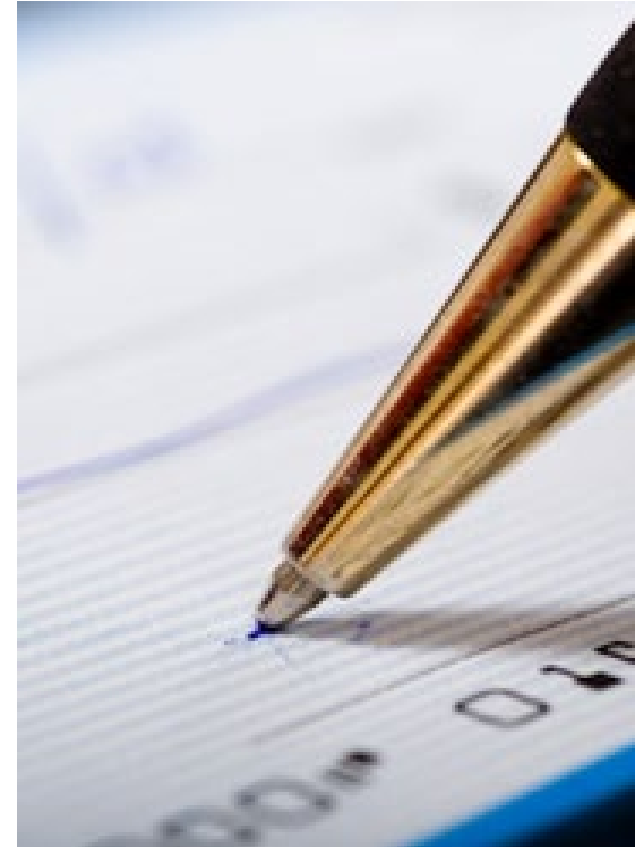
Fraudulent checks/deposits



- Significant increase in both frequency and severity of losses
- Deploying tactics from well-known social engineering schemes
- Money mules continue to assist
- Stolen mail has been the key driver



- Steal members' issued checks and alters them or manufactures fraudulent checks using info from legitimate checks
- Recruit money mules to open accounts, including business accounts, at credit unions to cash stolen and other fraudulent checks
- Open fraudulent business accounts in the name of the payees listed on the stolen checks



Fraudulent checks clearing member accounts

What's happening?

- Fraudsters steal members' issued checks from blue drop boxes
 - Alter/wash checks (payee)
 - Manufacture fraudulent checks using the information from members' legitimate checks
- Frequently deposited at ATMs or via remote deposit capture
- Withdrawals often take place at ATMs, casinos, or through Zelle/CashApp

- Credit unions can recover losses from members' altered checks (as well as checks containing a forged endorsement)
 - Pursue a breach of presentment warranty claim under UCC 4-208 against depository institutions that accept members' altered checks
- Credit unions typically take the loss from fraudulent checks created using information from members' legitimate checks
 - Checks must be returned by the credit union's midnight deadline



Some financial institutions are denying credit union breach of presentment warranty claims

- In many cases, they're incorrect
- Be persistent – make 2nd & 3rd requests
- Consider threatening legal action, if necessary
- These financial institutions will typically return the funds to the credit union

1. Pursuant to UCC § 4-208, the check is counterfeit/washed/traced or was not otherwise signed by an authorized signer of the drawer. The signature of the client on this check is not similar to the signature on other items we have pulled drawn by the maker, your customer. You, as the paying bank, had a responsibility to verify the signature. Because the signature is questionable, we decline to pay the claim.

Digitally-altered checks

- After stealing a member's issued check, fraudster scans the item, digitally alters the payee and prints it out on commercially available check stock
- Courts have ruled that digitally altered checks are more like counterfeits
- Counterfeits must be returned by the credit union's midnight deadline
- To have a valid breach of presentment warranty claim the original check must be physically altered



RISK Alert

Actionable insights for bond policyholders



Awareness

Watch

Warning

Altered checks: what you need to know

There has been a significant increase in members' issued checks being intercepted in the mail and either physically or digitally altered by fraudsters. The method used by fraudsters to alter the checks determines whether the credit union can pursue a presentment warranty claim under UCC 4-208 against a depository institution that accepts the check.

Alert details

The stolen mail problem has resulted in a significant increase in members' issued checks being intercepted and altered. Credit unions can attempt to recover losses from members' altered checks by pursuing a breach of presentment warranty claim under UCC 4-208 against the depository institutions that accepted the checks. However, the method used by fraudsters to alter the checks determines whether the credit union can pursue a claim against a depository institution that accepts the check.

When fraudsters intercept a member's issued check, they typically physically or digitally alter the check.

Physically alter/wash the payee and/or dollar amount - Using common household chemicals, fraudsters remove the payee and dollar amount while leaving the drawer's signature intact. The washing process essentially turns the check into a blank signed check on which the fraudster inserts a new payee and dollar amount.

Credit unions can attempt to recover losses from member checks that are physically altered/washed by pursuing a breach of presentment warranty claim under UCC 4-208 against the depository institutions that accept them.

Digitally alter the payee and/or dollar amount - A fraudster can scan the check, digitally change the payee and/or dollar amount using editing software, and print the item using commercially available blank check stock. Digitally altered checks often have:

- Inconsistent font styles, size and spacing in the payee's name and dollar amount (courtesy/numerical and written amount).
- Text that does not align evenly on the line.
- Logos that appear blurry or pixelated.

The courts have ruled that digitally altered checks are considered counterfeit checks because they don't involve physical modification of the original paper checks. The losses for digitally altered checks fall on the institutions on which the checks are drawn as they must return counterfeit checks by their midnight deadline.

Date:
June 2, 2026

Risk category:
Check fraud; Altered checks; Counterfeit; Deposit account fraud; Compliance

States:
All

Share with:

- Accounting
- Executive management
- Front-line staff/Tellers
- Legal/Compliance
- Member services/New accounts
- Risk manager
- Teller supervisor
- Transaction services



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

When fraudulent checks clear a member's account

Specific controls:

- Open new account with new account number and freeze old account
 - Request list of outstanding checks from member
 - Manually clear the checks against the old account as they're presented for payment
- Determine if the member reported the unauthorized checks within the timeframe outlined in the account agreement
 - Don't recredit member if reported late
- If applicable, pursue a breach of presentment warranty claim against the depository institution

General controls:

- Perform manual review of large dollar checks (e.g., \$10,000 or more) presented for payment
 - Verify member signatures against reliable specimens (e.g., signature card or loan documents)
 - Call member to verify that they issued the check to the stated payee for the amount listed
 - Check the member's account to make sure the phone number was not changed in the last 60 days before making the call
 - Review must be performed timely to allow the credit union to return unauthorized checks by their midnight deadline
- Consider offering payee positive pay to business members

Fraudulent business accounts

- Fraudsters - or their money mules - open fraudulent accounts, including business accounts, to cash stolen and other fraudulent checks
- Opens the account in the name of the payee on the stolen check, or alters the payee listed on the check replacing it with name
- Fraudsters file fraudulent articles of incorporation or similar document with the secretary of state and provide this document to the credit union at account opening
- Credit unions receive a breach of presentment warranty notice from drawee institutions claiming credit unions accepted checks containing a forged endorsement, or accepted altered checks

Red flags

- Payee's address on the check bears no relationship with the address used to open the fraudulent account
- Articles of incorporation or similar document filed with secretary of state just days before the fraudulent business account is opened
- Stolen checks are dated 3 to 8 weeks before the date of filing stamp on the articles of incorporation or similar document
- Business name listed as payee on the check may not exactly match the name of the fraudulent business account

Fraudulent business account

\$549k loss impact

- Money mule opened a fraudulent business account at a credit union located in MI on 7/12 to cash a \$549K stolen check
- Account opened in the name of the payee on the check
- Provided fraudulent registered articles of incorporation - filed 6/26
- Funds withdrawn through various means after the check hold expired
- Credit union received a breach of presentment warranty claim from the bank on which the check was drawn

Red flags

- Payee's address listed on the check was Chicago – account opened using a Michigan address
- Articles of Incorporation filed 6/26
- The check was dated 6/12



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



Risk mitigation – fraudulent business account

- Deploy identity verification solution to verify the identity of beneficial owners
 - Verify business entities by obtaining registered articles of incorporation
 - **Be wary of recently filed articles of incorporation**
- Do a search on the business name
 - Place extended holds on checks deposited to new accounts in accordance with Reg CC
 - Consider establishing a waiting period before new members can use remote deposit capture service

Kiting indicators

- Frequent deposits of even dollar amounts and subsequent share draft withdrawals in the same or similar amounts
- Business member deposits checks that are drawn on their account from another financial institution
- Checks are typically drawn on an affiliated business under the control of the business member
- Kite may involve multiple affiliated businesses with accounts at different financial institutions
- Deposits of increasing dollar amounts
- Excessive deposits made at ATM, night depository, or using remote deposit capture
- Frequent NSF deposits/frequent share draft overdrafts



Fraud trends on the radar

Card fraud



Card fraud: BIN attack or brute force attack

What's happening?

- Experimental method in which fraudsters attempt to identify valid card numbers by use of data-collecting software
- Testing each card 1-2 times per day

Signs of attack

- Large volumes of transactions at a single merchant
- Transaction amounts from zero dollars to under five dollars
- High volumes of denial for CVV2 failure or invalid account number
- Incorrect expiration date

Mitigation tips

- Review reports to monitor unusual high volumes of transactions
- Block high risk merchants
- Randomize your card numbers and expiration dates
- Utilize 3D secure 2.0 for online purchases
- Work with card processor to set rules and strategies to detect and prevent BIN attacks
- Encourage members to use card transaction alerts and report unauthorized activity immediately



Card provisioning & tokenization

- Provisioning adds a card to a digital wallet through manual entry, card scanning or in-app push provisioning
- Tokenization replaces the PAN with a unique digital identifier during transactions
 - Require multi-factor authentication and biometric verification before provisioning cards
 - Use device fingerprinting, geolocation, and velocity controls to detect suspicious activity
 - Provide real-time member alerts and self-service tools to manage or revoke wallet tokens
 - Monitor token activity and maintain controls throughout the entire token lifecycle to reduce fraud risk
 - Ensure tokenization is implemented for wallet & stored credentials; review token lifecycle



Provisioning & Tokenization of Mobile Wallets Checklist



Using a digital wallet like Apple Pay®, Samsung Pay or Google Pay™, your member can make secure contactless payments at checkout. These digital wallets use the same tap-and-go technology as contactless cards and can be used wherever contactless cards are accepted, with the added benefit that higher value purchases can be made, because you authenticate yourself on your device before you tap.

In-app provisioning and digital tokenization are two important concepts with mobile payments and digital wallets.

The combination of in-app provisioning and digital tokenization offers several benefits, including:

- Enhanced security by reducing the risk of fraud
- Improved user experience by adding cards to mobile wallets streamlining the payment process
- Increased adoption and driving growth for payments
- Reduced complexity and expenses associated with multiple integration efforts

What's the difference?

Provisioning

In order to use mobile payments, a virtual card or account needs to be provisioned. Provisioning covers the process of preparing and loading an application onto a user's phone with personalized account data.

Provisioning adds a payment card to a digital mobile wallet such as manually entering card details, taking a photo of the card, or using an in-app "push" method within an issuer's app.

Tokenization

Replacing the card's sensitive account number with a unique, non-sensitive digital identifier is called tokenization where a token that is saved in your phone, watch, or the merchant's site where your member registers their card. This security measure makes mobile payments safe by protecting card data.

Tokenization protects your members' account by using that token instead of their real card number, which the merchant never sees or stores.

Fraud trends on the radar

Wire fraud: fraudulent instruction & business email compromise





Nearly 75%
of organizations
experienced email
or business email
compromise fraud

Source: Payments Fraud and Control Survey Report,
2026 Association for Financial Professionals

\$3.05 billion
in adjusted losses
from business email
compromise fraud

Source: IC3 2025 Internet Crime Report, FBI

Business email compromise

- Typically involve an executive level employee's email or phone number that has been compromised or spoofed through a phishing attack
- Fraudsters hack credit union CEO's email – searches for email exchanges with another executive
- Fraudster may write email rule to send all incoming and outgoing email to the CEO's trash folder
- Fraudster usually sends a spoofed email – appearing to come from the CEO – requesting a large dollar wire to pay a vendor or purchase investment
- May send the email from within the CEO's hacked email account
- Usually involves a **sense of urgency** and/or is aligned with the executive being **out-of-office**



Loss case studies

- Credit union was remodeling a location
- CEO's email was hacked – fraudsters found email exchanges with contractor in charge of the remodeling project
- Fraudster sent several spoofed emails to accounting manager to pay contractor's invoices via wire
- Initial loss was nearly \$10 million
- Credit union was able to claw back \$7 million
- Credit union impact: **\$3 million loss**

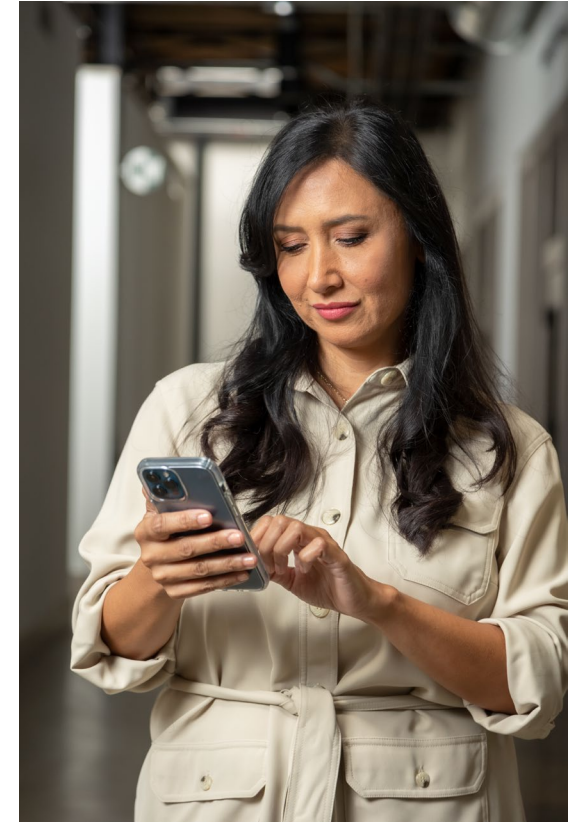
- CEO's email was hacked – fraudster found email exchanges with CFO
- Fraudster created email rule to send all incoming and outgoing email to trash folder
- Fraudster sent email to CFO from within the hacked email account requesting a \$500K wire to purchase an investment while CEO was out of the office
- Fraudster sent another email to the CFO the next day requesting a \$1.5 million wire
- Second wire didn't go through as CEO confirmed she did not send the email
- Credit union impact: **\$500K loss**

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

Business email compromise

Loss case study

- Credit union CEO's Office 365 account was hacked
- CEO received phishing email purportedly from the credit union's legal counsel with a legal document attached (CEO was expecting this document)
- To open the attachment, the CEO was required to enter their Office 365 login credentials (captured by fraudster)
- Fraudster sent email to the CFO from within the hacked email account requesting a \$960K wire
- CFO attempted to authenticate the CEO's request by messaging them through Teams, but the fraudster acknowledged the request, so the wire was executed
- Sending a Teams message to the CEO is not an out-of-band method (it's a part of Office 365)
- Good news! Credit union recovered \$950K from the bank



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

Deepfakes

- Fraudulent activity becoming more convincing with AI-generated audio and video capabilities
- People saying and doing things they didn't
- Gamechanger for business email compromise and impersonation fraud
- Additional potential impact:
 - exploiting member onboarding processes
 - creating fraudulent accounts, counterfeit payment or transfer requests
 - mimicking job candidates

Unfortunately, conventional security technologies & identification protocols are designed to identify impostors - not recognize altered or recorded voices or digitally enhanced and manipulated videos

Deepfake fraud attempts have grown significantly over the last three years

Deepfake loss case studies

- Fraudsters cloned a company director's **voice** in a \$35M fraud scheme
 - Branch manager in the company's office received a call from the company's director – a voice immediately recognized
 - The director informed the branch manager the company was going to acquire a business and the branch manager needed to make \$35 million in wire transfers
 - Believing the instructions were legitimate – based on recognizing the director's voice – the branch manager executed the transfers
- Fraudsters used deepfake **videos** to con a finance employee of a multinational company to transfer \$25M
 - The con featured deepfake videos of the CFO and other employees, **who were all known to the finance employee**, in a live video conference call
 - The CFO instructed the finance employee to make a \$25 million wire transfer
 - Believing the instructions were legitimate – based on recognizing the CFO and other employees in the video conference call – the finance employee executed the wire

Risk mitigation: Use an out-of-band method to verify internal wire requests no matter how they are received – by phone (voice message or live call), email, and live video conference calls.



Top things to consider

- Do not assume a phone call, email, text message or video clip is genuine
- Foster a zero-trust environment by encouraging employees to be suspicious – add email warning messages
- Enable robust security controls, two-factor authentication, and strong login credentials
- Explore AI and liveness detection software to detect deepfakes

The risk isn't just the technology, but rather people's natural inclination to believe what they see and hear.

Risk resources

Business Protection Resource Center www.trustage.com/bprc

- RISK Alerts – warning | watch | awareness
- Loss prevention library
- risk overviews, checklists & whitepapers
- Emerging risks outlook
- Live webinars, risk forums & office hours
- On-demand learning & interactive training modules

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

Executive Vice President - \$3B credit union



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 into 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.

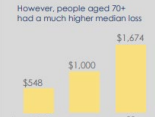
You can report fraud, scams, and other illegal business practices by going to the Federal Trade Commission website: www.ReportFraud.ftc.gov

Younger people lost money to fraud more often than older people

43%
Victims ages 30-39 lost money to fraud

23%
Victims ages 70-79 lost money to fraud

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





Account takeovers

Risk overview



Losses from account takeovers of member accounts have increased significantly in frequency and severity in recent years. Several credit unions have incurred seven-figure account takeover fraud losses.

Account takeover is a type of identity fraud where fraudsters leverage a person's existing credentials to take control of their legitimate financial, credit, email, or social media accounts. This unauthorized access to user accounts can lead to various account takeover attacks.

Unfortunately, just about every type of industry that holds sensitive data is at risk of account takeover-based fraud.

Fraudsters have launched sophisticated social engineering attacks against credit union members to scan them into providing their online banking login credentials, including two-factor authentication passcodes.

How account takeovers happen

There are a variety of methods used by fraudsters in their account takeover efforts, including:

- Social engineering
- Phishing, smishing & vishing
- Brute force attacks
- Credential stuffing
- Malware
- Man-in-the-browser attacks
- Application flaws

Losses from account takeovers can escalate very quickly as fraudsters can potentially target a very large number of members every day over the course of consecutive days. A credit union could potentially incur thousands of dollars in daily losses.

The dark web has made account takeover fraud much more attractive to attackers by reducing liability as they no longer need to steal directly from targeted users. Fraudsters can simply purchase valid login credentials instead of performing the time task of cracking passwords. The network of increased online financial accounts and offerings also fuel account takeovers.

A significant negative impact is having member accounts drained by fraudsters and their fraudulent transactions. However, these financial losses can also bring on significant organizational reputation damage and potential legal ramifications due to data security and protection of personal data.



RISK Alert

Actionable insights for bond policyholders



Awareness

Watch

Warning

ITM fraud takes on new twists

Interactive Teller Machine (ITM) fraud remains a significant challenge with reported losses reaching seven figures. Criminals are exploiting the ITM self-service functionality without the assistance of a live virtual teller.

To compound ITM risks, fraudsters are now employing social engineering tactics to deceive members into revealing or verifying personal information to gain access to audio phone banking or online banking. Once obtained, fraudsters change the PIN, initiate large dollar member-to-member transfers between victim accounts, and withdraw the money through the ITM by entering account numbers and audio-response PINs.

Alert details

As more credit unions deploy ITMs, fraudsters are identifying vulnerabilities to access member accounts. These ITM attacks often occur late at night into the early morning hours on weekends to avoid detection. A key weakness fraudsters are now exploiting is the use of a member's account number and audio response PIN for ITM authentication.

Initially, fraudsters accessed and withdrew funds from members' accounts — such as home equity line-of-credit loans (HELOCs), money market accounts, and other high-value accounts — by taking advantage of authentication processes that relied on easily identifiable information including account numbers, Social Security numbers, and dates of birth. Another tactic involved creating counterfeit debit cards to gain unauthorized access.

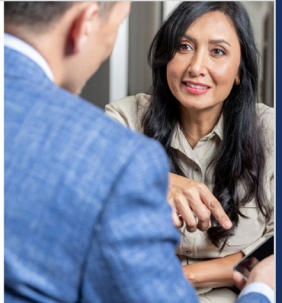
However, more recently, fraudsters have turned to social engineering tactics. By spoofing the credit union's phone number, they contact members under the guise of investigating suspicious transactions. Armed with limited personal information — such as the last four digits of a social security number — they scam or conjoin ITM self.

With this response, can initiate victim number.

Risk & Compliance Solutions | Presentation

Emerging risks outlook

Rethinking protection in an era of uncertainty





Related links & resources you may find helpful

Business Protection Resource Center @ www.trustage.com/bprc

- [RISK Alerts Library](#)
- [Loss Prevention Library](#)
- Need access to Resource Center or not receiving Alerts
>>> [step-by-step instructions](#)

"I appreciate that RISK Alerts, articles, and resources are included. It makes it easy to access and extremely efficient."

Risk Manager - \$1.1B credit union

"You all make it very easy to keep up with the latest technology and risk involved."

Director of Fraud Prevention - \$2.5B credit union



Key emerging risks & loss trends

TruStage

Key loss trends

risk overview – midyear 2026

Credit unions are facing a rapidly evolving risk environment characterized by increasing loss severity, more coordinated fraudulent attacks and greater adaptability by fraudsters. The average reported TruStage credit union loss in 2025 was \$1.1M, compared to \$1.0M in 2024.

TruStage

Let's Talk emerging risks

While each organization has its own unique risk footprint, risks are rapidly evolving and so must the strategic conversation with risk and compliance in mind. Unfortunately, risks and losses fluctuate at the same time, bad actors produce new innovative tactics and schemes.

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

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

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

Emerging risks are often categorized

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

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

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

CRITICAL LARGE LOSS PATTERNS

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

- **Account takeovers**
Fraudsters use sophisticated social engineering attacks against members to scam them into providing their login credentials, including two-factor authentication passcodes.
- **Fraudulent checks clearing member accounts**
Stolen mail has resulted in a significant increase in fraudulent checks clearing member accounts. Fraudsters steal members' issued checks and alter them or manufacture fraudulent checks using the info from members' legitimate checks.
- **Fraudulent deposits / U.S. Treasury checks**
Fraudsters frequently recruit money mules to open accounts at credit unions to cash stolen or fraudulent checks, including Treasury checks. They also open fraudulent business accounts in the name of the payees listed on the checks.
- **Interactive Teller Machine (ITM) fraud**
Fraudsters use the self-service feature to withdraw funds from member accounts – primarily using counterfeit debit cards. In some cases, deep insert skimmers were found on ITMs.
- **ITM / ATM jackpotting**
These cases involve fraudsters installing malware via the ATM top hat, connecting a black box device, or through remote network attacks. Once installed, fraudsters issue a command to dispense cash immediately or at an opportune time.
- **ITM / ATM smash 'n' grab**
A resurgence in ATM burglaries where criminals use a blow torch or other forced entry to open the ATM's money chest or steal it altogether.

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



Thank you.

Contact

riskconsultant@trustage.com

800.637.2676

This presentation was created TruStage based on our experience in the credit union and insurance market. It is intended to be used only as a guide, not as legal advice. Any examples provided have been simplified to give you an overview of the importance of selecting appropriate coverage limits, insuring-to-value and implementing loss prevention techniques. No coverage is provided by this presentation/ publication, nor does it replace any provisions of any insurance policy or bond.

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.