TruStage™

Call center fraud

Risk overview

Inbound call or contact centers are increasingly considered the key "soft" targets for fraudsters who impersonate legitimate members to alter or obtain information. This information is then used to facilitate direct and cross-channel fraud, which can be very difficult to tie back to the call-center entry point.

Regardless of the channels scammers use to conduct fraud, the call center typically plays an important role at some point. Call center agents are often exploited by the scammer to deliver sensitive member details that can later be used in account takeovers or other illicit activities. And in some cases, fraudsters will leverage a financial institution's call center to commit application fraud on the spot.

Common types of call center fraud

- Account takeovers - once fraudsters gain access to it, they can take over the account and change critical details that lock out the real user.
- Impersonating members to withdraw funds, request wires, change beneficiaries, and request new credit / debit cards.
- Social engineering call centers to change member contact information (usually a part of a wire fraud scam; or the fraudster requests HELOC checks, or orders share drafts on a member's account).
- Fraudsters can gain the information they need through the call center, then use it elsewhere to create credit applications, make purchases, and conduct other illicit activities.
- Fraudulent requests for HELOC advances (to fund a fraudulent wire request, counterfeit / forged share drafts, or fraudulent transfers made through online banking).

> 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 often use emotional appeal. They look to succeed by tugging at your basic human instincts to please, hope to catch you off-guard, and dupe you to comply with instructions from a malicious actor, and get you to act quickly.

Regardless of the fraud type or intention, the scammers' first objective is to convince a call center representative that they are a real member.

From new enrollment, to changing account information, to completing transactions, call centers are often the first and, in many cases, preferred point of contact for members wanting do business with the credit union.

While fraudsters attempt to infiltrate every industry and multiple organizations within an industry, any customer / member can become the victim of call center fraud. Not surprisingly, call center fraud is on the rise.

Fraudsters love to take advantage of times of disruption ,confusion and high emotion - and with financial institutions having to quickly adjust to working from home — distractions and security risks follow. Bad actors know call centers are often stretched thin, and they use that to their advantage.

The call center is often a first stop for fraudsters

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.

Call centers are also unique because of the human element involved — call center reps are expected to deliver a consistently positive member experience and simultaneously perform first-line fraud defense. That is a difficult balance in today's customer-centric environment.

Fraudsters will often start in the call center, and then move on to digital channels. Once a fraudster takes over a victim's account via the phone channel, the fraudster may change an online banking password and phone number associated with that account. This sets the stage for fraudsters to steal funds from the accounts.

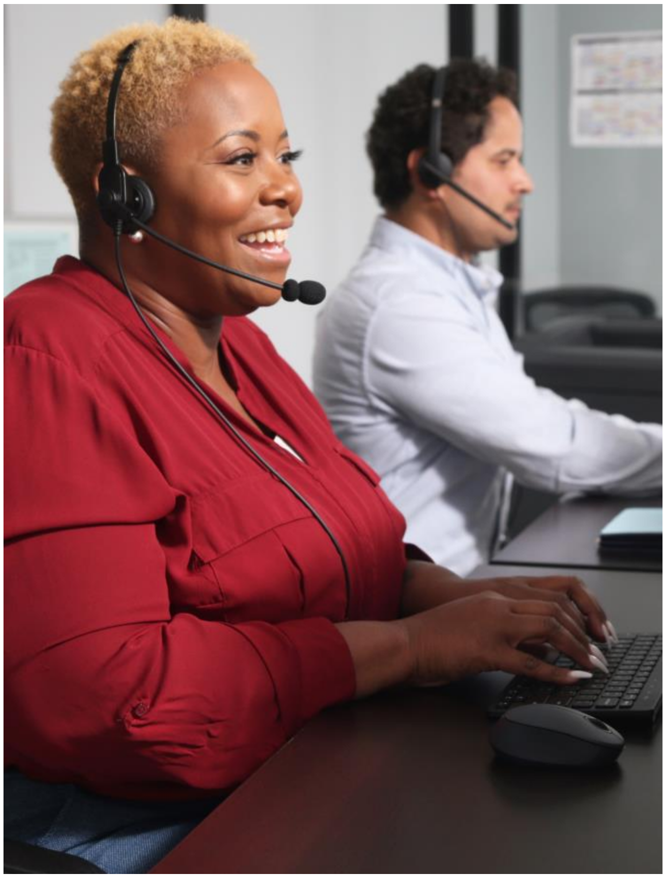
Nearly two-thirds of financial services organizations are concerned about fraud originating from contact centers.

Source: Neustar, 2021 State of Call Center Authentication

Fraudsters attack on multiple fronts

To combat call fraud and account takeover attempts, call centers must be able to detect two kinds of fraudulent activity:

- call spoofing to impersonate customers, and
- the use of virtual call centers to launch anonymous attacks.



Call center fraud characteristics

Mitigating fraud is a persistent challenge for many financial institutions. Fraud schemes continue to shift and evolve, leaving your business fighting an enemy best characterized by a formidable trait: constant change. These are some characteristics that your call center should be weary of:

Fraudsters can be friendly

It's natural to think of a fraudster as a shady character working alone in a dark room. Yet, fraudulent activities are often generated from large-scale boiler rooms where individuals are trained to develop emotional and personal connections to manipulate call center representatives. This approach unfortunately causes many to take actions that are not in the best interest of members.

Phone numbers can be spoofed

Most call centers have caller ID, and the phone number that appears is one source of identification. Unfortunately, this can trip up call center reps who let their guard down when a call appears to be coming directly from a member's phone number. Additionally, phone technologies have become more advanced, more affordable, and readily available for fraud organizations to use to their advantage.

Forms of ID are easy to steal too

Fraudsters often call into call centers prepared with stolen account numbers, phone numbers, addresses, dates of birth, and Social Security numbers. Therefore, it's important for call center representatives to watch for unusual requests such as out-of-the-country transfers, changes of addresses and passwords.

In addition, more states have considered or implemented digital driver's licenses and IDs. The convenience of a digital license may not be harmful, but some argue that personal data on a phone may be too risky. The software isn't always the softest target…it is often the people using it.

Beware of telephony flooding attacks

Fraudsters will sometimes use the tactic of trying to overwhelm and confuse call center representatives with a flood of calls at one time. If this type of flooding of the phone lines begins to happen, representatives should be armed with the ability to alert management.

Most account takeovers are believed to begin through this channel at financial services organizations:

38%	38%	17%
website	call center	mobile application

Source: Neustar, 2021 State of Call Center Authentication

Confronting call center fraud

Managing the risks of account takeovers requires a layered security program. That's why there is growing movement to using multifactor authentication, such as two-factor authentication and biometrics in the call center.

Layered security controls are characterized as different controls at different points in the transaction process so that if one control is defeated, another one exists that could help prevent unauthorized transactions.

Staying vigilant and implementing more versatile, risk-responsive authentication workflows can go a long way in protecting your business and promoting a frictionless interaction for legit members.

Two-factor authentication

Two-factor authentication or out-of-band authentication typically leverages the use of one-time-passcodes (OTPs) to authenticate a member attempting to access account information or perform a transaction. OTPs are generated and typically delivered to the member via automated phone call, email, or SMS text message. Members usually have a choice in the delivery method using the contact information the credit union has on file.

However, fraudsters have easily intercepted passcodes using these delivery methods (phone call, email, or SMS text message) – primarily through hacking email accounts and/or social engineering tactics. Deploying a more secure two-factor method, such as a passcode generating token (hardware of software) has proven to be more reliable for many credit unions.

Two-factor authentication is considered a "must-have" control to help mitigate the risk of account takeovers and controlling social engineering fraud.

According to the State of Call Center Authentication study, most respondents (83%) overwhelmingly want to keep call center representatives out of the authentication process. The preference for the call center journey is that the caller completes authentication pre-answer or while a caller engages with an interactive voice response (IVR) system.

Minimizing human involvement in authentication can provide less opportunity to socially engineer call center reps into granting illicit access to member accounts.

Confronting call center fraud

Knowledge-based authentication

Knowledge-based authentication (KBA) is only as strong as the identity intelligence your business uses to perform KBA. Performing KBA with information that is readily available (e.g., name, address, Social Security Number, account number) to fraudsters via recent breaches, social media sites or simple internet searches is ineffective and inefficient.

Examples of strong knowledge-based questions include:

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

To perform adequate KBA you need access to enhanced identity intelligence that is built from multiple sources that are frequently updated. Utilizing robust data sources that aren't readily accessed by the public is essential. The best practice for KBA is an analytic-based solution that can create dynamic, risk-responsive questions in real time.

An additional layer of fraud protection can be accomplished by authenticating a device at the beginning of a customer interaction. Verifying the full device identity and location attributes can provide essential information that could be used to uncover a fraud attempt or flag an interaction for additional authentication protocols. In the case of the call center, understanding the device identity and location can help call center agents confirm the device belongs to the caller, detect call spoofing attempts and understand if any fraudulent or suspicious activity has been associated with the device.

Voice biometrics

A useful element of layered security is voice biometrics that can capture fraudster voices by comparing them with legitimate voice prints of members. Voice biometrics create an additional level of authentication that, unlike fingerprints or facial recognition, easily translates to the call center level. An ideal voice biometric solution is designed to help promote a positive member experience and prevent implementation delays and technology roadblocks.

Voice biometrics uses voice patterns and characteristics to produce unique identification for every individual, typically using hundreds of physical and behavioral factors. These factors can include pronunciation, emphasis, speed of speech, accent, as well as physical characteristics of your vocal tract, mouth and nasal passages. The drawback is you have to capture the member's legitimate voice before being able to use.

Fraud monitoring solution & predictive behavioral analytics

Curating user behavior analytics can help organizations better understand how users legitimately interact with their information systems and data versus how a malicious attacker would behave.

User analytics have the potential to increase early threat detection. For example, analytics could recognize that a user is behaving differently than in the past, which could indicate his or her credentials have been compromised and are being used by someone else.

Artificial intelligence and machine learning have become so prevalent that many businesses now heavily rely on algorithms to make decisions that can impact our daily lives, including member service interactions.

Confronting call center fraud

Phone printing technology

Just like your fingerprint, your call audio has a unique signature. Whenever you pick up the phone, your device, your carrier, your geographic location, and your network routing contribute very subtle audio characteristics to your call. These traces of valuable information are invisible to most people - and it's important to note that, unlike your voice or your phone number, you can't manipulate, spoof, or otherwise disguise them. Phone printing solutions can be extremely effective at preventing call center fraud.

- Phone printing can detect caller ID spoofing by comparing caller ID information to the true device and geolocation to spot anomalies that indicate spoofing.
- Phone printing can detect the geolocation where the call originates. For example, let's say a fraudster in an eastern European country calls the credit union and impersonates the member. Phone printing will tell you where that call originates. Definitely a red flag.
- Phone printing can detect the type of device used to make the call – such as a mobile phone, landline, or Voice over Internet Protocol or VoIP.

Phone printing provides universal protection for all calls within the call center which allows you to identify unknown attackers on their first call, while also creating a list of known attackers, based on phone number, phoneprint, and voiceprint.

The risk of deepfakes

Deepfakes are digitally-altered images, videos, or audio recordings that when using certain technologies, can convincingly make it appear an individual said or did something they didn't do.

Initially used to impersonate politicians, celebrities, and other well-known individuals; the technology has become increasingly available to fraudsters and other bad actors and deepfakes are now being used in social engineering attacks for fraudulent financial gain.

As some credit unions have pivoted to the use of photographs or "selfies" with government-issued ID's as well as the adoption of voice recognition software for member identification purposes, impostors can use deepfake technologies to successfully bypass these new protocols.

- Explore artificial intelligence (AI) and liveness detection software to identify and alert your staff to potential attacks.
- Implement employee training and awareness as a critical component of defense in a credit union's deepfake mitigation strategy. Training programs should be centered on how the technology is leveraged in various malicious attempts, detection techniques, and enable reporting protocols for employees.

Targeting call centers to fraudulently wire funds

Fraudsters are frequently defeating identity verification solutions that rely on questions derived from member credit reports as well as out-of-wallet questions. These losses can easily reach six-figures – particularly when they are funded via unauthorized advances against member HELOCs.

Typical scenario:

- Fraudster calls the credit union to have the member's phone number changed on the account.
- Fraudster calls the credit union again, this time to request an advance against the member's HELOC depositing the funds to the member's checking account.
- Alternately, the fraudster activates telephone banking on the member's account to take an advance against the HELOC.
- Fraudster calls the credit union to request a large dollar wire transfer.
- Credit union performs a callback verification; however, the call is made to the changed telephone number which is controlled by the fraudster. The fraudster successfully answers the security questions.
- Credit union executes the wire

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

Train employees to recognize psychological methods that social engineering fraudsters use:

- power
- authority
- enticement
- speed
- pressure

Prior to performing a callback verification, review the member's account to determine if the phone number was changed within the last 60 days.

If the member's phone number was recently changed, require the member to complete the transaction in-person.

Common red flags

- Member calls several times in a short period of time
- Requests to change information on file such as the address and/or phone number
- Caller redirects conversation when unsure of answers regarding authentication
- Long pauses or incorrect verification answers
- Sets up member accounts for audio response and/or online banking
- Asks how to wire transfer money and/or requests wire transfers to foreign organizations

Is outsourcing an option?

The decision to outsource all or part of your call center can have far-reaching consequences.

The risks of outsourcing include loss of control; compromised service quality; violating regulatory compliance; and communication barriers.

Tips for mitigating outsourcing risk:

- Clearly define your objectives
- Develop a robust selection process
- Be thorough in your due diligence
- Transparent communication benefits both partners
- Don't base your decision solely on price

Be diligent in developing a strong compliance program. Not only will it potentially save your organization a lot of expense on possible penalties and remittance, but it can lead to increased transactions, conversions, improved member satisfaction, and stronger brand reputation.

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^{TM} Risk Consultant by contacting us at **riskconsultant@trustage.com** or at **800.637.2676**.

Fraudsters love call center agents because they are trained to be helpful. This makes contact centers an attractive target. With the continuous evolution of fraud, the demand for detection and prevention solutions is critically needed.

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. TruStageTM 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.