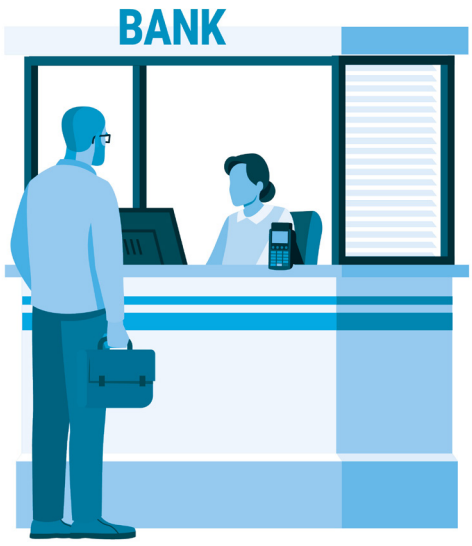
ACCOUNT TAKEOVER FRAUD: DETECTION AND PREVENTION BY CHANNEL

Criminals exploit every available access point (e.g., branches, call centers, email/SMS, and online/mobile banking) to impersonate legitimate account holders and execute account takeover fraud. Because their tactics shift depending on the channel, an effective defense strategy benefits from channel-specific controls. The following sections outline different prevention and detection approaches that financial institutions can consider implementing for each channel.

IN-PERSON (LOCAL BRANCH)

Although less scalable than digital attacks, criminals still take advantage of in-person interactions to impersonate legitimate account holders and gain unauthorized access. They may present forged or altered identity documents, rely on partial but accurate personal information, or attempt to manipulate and pressure staff into bypassing established verification controls.



Scenario: *A "customer" walks into a branch near closing time, claims an urgent need to replace a lost debit card for a large purchase, and accurately provides the account holder's name and phone number. He encourages financial institution staff to bypass a secondary verification step for replacing the lost card. When the employee does not initially comply with his request, he threatens to take his business elsewhere if not accommodated.*

PREVENTION AND DETECTION APPROACH	WHAT IT DOES
Educate staff on social engineering	Helps staff recognize attempts at emotional manipulation and soliciting exceptions
Implement enhanced identity verification for high-risk activities	Increases assurance around address or phone number changes, password resets, debit card replacement or large value transactions
Use document authentication tools/technology solutions	Helps staff identify potentially forged or altered IDs
Monitor for anomalous branch activity (e.g., atypical customer branch location, unusually large withdrawal request)	Flags customer behavior that deviates from what is normally expected at a branch

ACCOUNT TAKEOVER FRAUD: DETECTION AND PREVENTION BY CHANNEL

PHONE (CUSTOMER CALL CENTER)

Like the branch environment, the customer support or call center is vulnerable because it relies heavily on staff judgment to detect red flags or unusual behavior. Criminals take advantage of this by using voice cues to build credibility and mask their identity through caller ID spoofing, voice alteration and Voice over Internet Protocol (VoIP) technologies.

Scenario: *A call center receives an urgent phone call from a "customer" that is stranded at an airport and in need of a password reset. The caller's audio is distorted and delayed, although the area code of the caller matches the area code of the account holder's number on file.*

PREVENTION AND DETECTION APPROACH	WHAT IT DOES
Standardize call center employees' responses to common criminal pretexts (e.g. "I'm traveling internationally" or "My phone was lost")	Can help reduce incidences where call center employees are persuaded to skip controls
Train staff on recognizing VoIP indicators (e.g., audio distortion, latency, odd vocal cadence)	Helps detect spoofed or anonymous callers
Leverage carrier and line intelligence	Uses telecom data to identify whether a phone number is VoIP, recently ported or associated with suspicious routing
Leverage STIR/SHAKEN (Off-site) caller ID authentication	Validates whether the originating carrier cryptographically attested that the calling number is legitimate
Monitor for multiple suspicious call attempts	Detects coordinated probing or scripted calls

ACCOUNT TAKEOVER FRAUD: DETECTION AND PREVENTION BY CHANNEL

EMAIL OR SMS (TEXT)

Criminals may impersonate an account holder by taking control of their legitimate phone number or email address, or by convincing financial institution staff that they are the customer communicating from a "new" contact point. In SMS channels, Tactics often include spoofing sender IDs so messages appear to come from the customer's known number or email address and using stolen personal information or fabricated identity documents in communications with the financial institution to make sensitive requests appear legitimate.

Scenario: *A front-office staff member receives an email from a customer about ordering new checks. The tone of the email seems odd, and the customer has never ordered checks before. However, the staff member verifies that the email is from the customer's email address on file and approves the request.*

PREVENTION AND DETECTION APPROACH	WHAT IT DOES
Verify email or SMS requests through a trusted channel	Prevents weak-channel resets and confirms legitimacy of sensitive requests
Prohibit multi-factor authentication (MFA) resets from email-only (or SMS-only) requests	Avoids exploitation of potentially unsecured channels
Train employees to review email and SMS messages for anomalies or social engineering indicators	Flags potentially compromised accounts or impersonation attempts
Monitor for lookalike email domains	Helps identify domain impersonation
Standardize staff workflow for identifying risky emails or SMS communication	Ensures that sensitive actions follow a controlled process

ACCOUNT TAKEOVER FRAUD: DETECTION AND PREVENTION BY CHANNEL

ONLINE OR MOBILE BANKING

As discussed in other modules, digital channels are a major target for account takeover fraud due to high volume and convenience. Common attacks include automated credential stuffing, abuse of password reset or account recovery processes, and SIM swapping.

Scenario: *A financial institution's digital support team receives an alert that a customer's online banking account has just been accessed from a new mobile device located in a different region than where the customer is typically located. Minutes later, the customer sends a message through the mobile app asking to reset their two-factor authentication settings because "their old phone stopped working."*

PREVENTION AND DETECTION APPROACH	WHAT IT DOES
Implement MFA and biometric login	Increases the difficulty for unauthorized users to access accounts
Encourage device fingerprinting	Identifies risky, unfamiliar or suspicious devices attempting to log in
Implement malicious bot detection	Can help prevent automated credential stuffing/brute force attacks
Monitor for SIM changes	Detects potential attempts to intercept one-time passcodes
Use behavioral analytics	Flags unusual user behaviors, such as atypical mouse movements, typing patterns or impossible travel patterns
Leverage account and transaction monitoring	Identifies unusual account behavior and potentially fraudulent transactions
Deploy customer alerts	Provides rapid notification to the customer to confirm or deny unusual activity

ACCOUNT TAKEOVER FRAUD: DETECTION AND PREVENTION BY CHANNEL

CROSS-CHANNEL DEFENSES

Preventing and detecting account takeover fraud requires building a layered defense across every channel where customers interact with the institution. But equally important is the implementation of cross-channel controls that connect activity across online, remote and in-person interactions. Because criminals frequently pivot between channels to appear legitimate, organizations should consider how to best identify behavior in one channel that contradicts behavior in another, or behavior that amplifies signals in another. Some risk signals may look harmless in isolation but are highly suspicious when viewed together.

Scenario: *A criminal gains access to online or mobile banking using stolen or phished credentials. Once inside the customer's account, she updates the contact information, enrolls a new device, and disables customer alerts. She then calls the contact center to initiate a large-value wire transfer.*

PREVENTION AND DETECTION APPROACH	WHAT IT DOES
Unified cross-channel monitoring and analytics	Helps detect coordinated cross-channel attacks earlier by surfacing anomalies that span multiple touchpoints and type of interactions
Consistent identity verification and authentication standards across all channels	Helps prevent attackers from exploiting weaker authentication steps in a single channel to gain broader access
Real-time customer alerts across multiple contact methods	Increases the likelihood that customers will see and respond to unauthorized activity quickly; prevents criminals from silencing or controlling a single point of communication during an attack

ACCOUNT TAKEOVER FRAUD: DETECTION AND PREVENTION BY CHANNEL

CONCLUSION

Account takeover fraud is a dynamic, multichannel threat that requires financial institutions to think holistically about risk. Strengthening each individual channel — branch, call center, SMS, and online/mobile — is essential, but it is only part of an effective defense. Criminals strategically pivot between channels to appear legitimate and exploit the weakest point, which means prevention and detection efforts must extend beyond isolated controls. By combining strong, channel-specific safeguards with cross-channel visibility, analytics, and consistent authentication standards, financial institutions can more effectively identify suspicious patterns that would otherwise go unnoticed. Building this layered, coordinated approach not only improves fraud prevention but also strengthens customer trust and resilience across the entire institution.

The account takeover fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.