transmit security

USE CASE

Account Recovery

Why Account Recovery Is Risky Business

Account lockouts and friction-filled account recovery steps frustrate customers, multiply support costs and lead to drop-offs. Difficulties multiply when customers forget their username, the email account they used or their own answers to pre-selected security questions. Moreover, account recovery bypasses the initial login, and bad actors seize the opportunity — turning account recovery paths into attack vectors.

Typically, if a customer remembers their username, they can get a password reset link or code sent to their registered email address or phone as a form of authentication, a possession factor. It's a tedious but easy process (if the link or code arrives), but it does not prove the customer's identity with a high level of assurance (LOA). If the user's email account or phone has been compromised, a bad actor could be recovering the account.

Account recovery is even riskier and more complex when a customer forgets or no longer has access to the email address or phone number linked to their account. In this scenario, the customer (or imposter) may be asked to answer security questions or submit a photo ID, online or in person. Guessable or compromised answers result in fraud, whereas identity verification, a more secure method, can result in higher attrition rates if the process is not automated and optimized.

Phishing-resistant authentication can solve many of these problems. But what if the user loses or replaces their device, which stored their biometric and private key? Most 'passwordless' solutions require a password to recover an account, which means it's still vulnerable to phishing and other account takeover (ATO) tactics. Even passwordless authentication that's truly password-free cannot prevent ATO fraud on its own.

This paper explores these challenges and how Transmit Security provides a dynamic, AI-driven account recovery solution that continuously assesses the level of risk and trust and adapts user flows by adding challenges or removing friction in real time. A unified platform simplifies and secures the entire process, minimizing risk, costs and churn.

Account recovery with Transmit Security

Transmit Security makes it easy for customers to recover their accounts while preventing criminals from exploiting the same process. Our platform addresses the complete use case out of the box — with a full set of account recovery methods to fit every customer scenario. You'll reduce support costs while optimizing user experiences (UX) and security.

For starters, our passwordless authentication is truly unique, enabling customers to recover accounts without ever using a password. The platform also strengthens and simplifies password-based recovery with a full range of authentication methods, AI-driven fraud detection and identity verification. Orchestration then correlates data and adapts user flows based on risk and trust, adding challenges or removing friction in real time.

For example, if a customer recovers their account with an email magic link or one-time passcode (OTP), our fraud detection engine passively verifies the user with behavioral biometrics and device fingerprinting. If there are signs of risk, orchestration can invoke another authentication method or ID proofing. Platform-native identity verification offers a simple, guided process that analyzes photo IDs and live selfies with supreme accuracy.

The challenges of account recovery

It's notoriously difficult to implement an account recovery process that prevents fraud without creating more friction for customers who are already locked out and frustrated. To get it right, it's essential to examine and address all of the issues:

Weak recovery methods: To secure account recovery, most companies use security questions, email reset links and/or SMS OTPs, but these methods are not foolproof for a variety of reasons:

- **Exposed security questions:** Answers can be phished or found online, like a mother's maiden name or childhood pet. To reduce risk, some create fictional answers, but this increases the chances they'll forget, which leads to higher support costs or drop-offs.
- **Reliance on email:** When sending a reset link or code, there's no guarantee the email is going to your customer. If a fraudster takes over an email account, it's a single point of failure that will allow the attacker to request reset links for all of the victim's accounts.
- **SMS OTP capture:** Attackers use banking trojans to intercept text-based OTPs or push notifications. Likewise, remote access trojans (RATs) steal OTPs, gaining access to a victim's OS, screen and keystrokes. Codes can also be intercepted by OTP capture bots, which often exploit application vulnerabilities. SIM swaps and man-in-the-middle attacks can intercept all communications, including security questions, email reset links and OTPs.

Phishing for credentials: Fraudsters often use password reset emails in phishing attacks, telling victims they need to enter their current credentials and then create a new password for security reasons. They also capture OTPs or security answers in the process.

All types of phishing attacks increased in 2023, rising 1,265% — largely attributed to generative AI (GenAI). With image generation and translation tools, fraudsters are creating flawless phishing campaigns that evade legacy detection and deceive more victims.

Voice deepfakes: The abuse of GenAI extends to call centers where voice cloning is able to dupe voice authentication systems, used by some companies as an account recovery method. With as little as three seconds of recorded audio obtained from phishing calls or online voice recordings, novices are able to create realistic deepfakes that pass voice authentication, even liveness checks.

Fake IDs: To strengthen account recovery, some companies now require a photo ID. But to pass identity verification, fraudsters use high-quality fake IDs, easily purchased or created online. Some services on the darkweb offer Photoshop-like tools that enable fraudsters to paste their own photo into a real ID template. Alternatively, they can use video deepfakes to pass liveness checks and facial biometric matching with someone else's ID. Both methods are able to deceive most online identity verification and manual screenings.

Vulnerable passwords: When resetting a password, a customer is just trying to get back into their account. This, combined with password fatigue, often leads them to set a weak password or reuse a password, so they can remember it next time. In turn, their account becomes more vulnerable to ATO fraud tactics, like brute force and credential stuffing. In 2022, stolen credentials accounted for 49% of all breaches.

Siloed detection engines increase error rates: To secure the entire user identity lifecycle, companies add disparate multi-vendor anti-fraud solutions, each with a narrow set of detection methods. When it comes to account recovery, security teams are left with data silos and blind spots, unable to see the full context of an account recovery request.

Analyzing a limited set of signals leads to mistakes; false positives disrupt customers and false negatives result in fraud. The consequences are costly. Adding to the challenge, fraudsters rapidly evolve their account recovery fraud tactics and mimic user behavior to evade detection. Risk assessments are clouded by the fact that customers occasionally deviate from their norm, logging in from a new location or device, for example.

Overhead complexity and cost: Stitching together various account recovery methods with multi-vendors solutions for fraud detection, identity verification and authentication adds complexity and costs. It requires difficult integrations, decision-making structures, coding and tuning cycles. Data correlation is further complicated by black box AI models. Costs continue to rise as you build and maintain layers of heuristic rules to detect new fraud MOs. It requires non-stop effort with suboptimal results.

Poor UX: Cumbersome account recovery processes create more friction than some customers will tolerate. As you invoke authentication challenges or identity verification, you may be adding barriers and complexity that lead customers to call support or drop off entirely. Detection errors that result in fraud or unnecessary friction further degrade UX. Either way, it's a bad experience that translates to lost revenue.

The cost of support and lost business: According to analysts, an estimated 20-50% of customer support requests are for help with account recovery, and each support call costs a company $70 or more. If the customer service experience itself is frustrating (e.g. they've forgotten their answers to security questions), the recovery process can negatively impact brand loyalty and customer retention.

Account Recovery with Transmit Security

Transmit Security provides the only risk-aware account recovery solution able to detect and mitigate risk or remove friction for trusted customers on the fly. A unified platform addresses the full use case out of the box — purpose-built to secure account recovery, optimize UX, reduce costs and increase revenue. This leading-edge solution includes:

Recovery methods to fit every scenario: With a full range of self-service account recovery methods and passive fraud detection in a single solution, customers can select the most convenient way to unlock their account while meeting your security requirements. Flexible, easy options offer multiple layers of protection.

A full set of authentication methods: Let customers recover their password-protected accounts with passkeys, passwordless, email magic links, OTPs, KBAs, social logins or any combination. Our service detects if the user already has passkeys or a biometric-enabled device and can prompt them to recover their account with phishing-resistant credentials. Account recovery is an ideal time to switch customers to a stronger, easier form of MFA.

Recovering phishing-resistant credentials: Customers who use our passwordless MFA can recover accounts with a high LOA without ever using a password. They simply transfer trust to a new device by scanning a QR code. To recover passkey-protected accounts, Transmit Security ensures keys only sync to devices when initiated by a deliberate transfer of trust. They can also recover passkeys with other authentication methods or identity verification, depending on your security requirements.

Real-time fraud detection: Behavioral biometrics, device fingerprinting, bot detection, and authentication analysis are among hundreds of detection mechanisms that run passively in the background to detect risk and trust throughout the account recovery process. By building complete user profiles, our risk engine has a 360° view of each customer and their devices, comparing typical behavior and device fingerprints to real-time activity, including mousing patterns, device integrity and travel velocity.

We've also developed robust malware detection models to stop new and evolving threats, including trojans, password reset overlays, keyloggers, OTP harvesting and other malicious behaviors. Transmit Security's holistic, contextual analysis delivers the most accurate risk scores, reducing false positives and false negatives by 90% when tested against other solutions.

AI-driven identity verification: When the highest LOA is needed, identity verification determines if the individual's photo ID and selfie are legitimate while minimizing friction. With Transmit Security, the customer only needs to submit a photo ID one time. For instance, if they've already done identity verification for account opening, they can later recover their account with just a selfie, which is compared to the ID previously provided.

- **Quick and easy UX:** Our UI guides customers through a simple process, using their phone to photograph their ID and/or a selfie. Results arrive in a few seconds.
- **Selfie authentication:** Biometric matching compares the selfie to the ID photo and a database of known fraud faces. Liveness detection spots selfies made with deepfake videos, photos or other tricks.
- **Deep document inspection:** Matches dates with templates, fonts, holograms and other features, using 150+ weighted analyses and ML to spot fake IDs. Global coverage supports 10,000+ government-issued photo IDs and is kept up to date. Our researchers also analyze new fake IDs and update ML and AI algorithms immediately.

Identity orchestration: Industry-leading orchestration pulls all of these capabilities together, eliminating the need for integrations — no coding required. Consolidation minimizes IT complexity and seals the cracks to prevent ATO fraud, even deceptive attacks that use device emulators, bots and fake IDs. This powerful engine delivers:

- **Out-of-the-box decisioning rules:** Orchestration correlates data across capabilities, apps and channels to view the full context of risk signals and accurately pinpoint suspicious activity. When anomalies are detected, real-time action triggers automatically adapt the account recovery journey based on a holistic view of risk and trust. Pre-made and customizable decisioning rules eliminate the cost and complexity of building and maintaining decision logic.
- **Drag-and-drop journey builder:** A visual, no-code journey editor makes it easy to build and alter account recovery flows across channels. Simply drag and drop elements to build secure and easy customer journeys, establishing if and when you need identity verification, passwordless authentication or advanced recovery combinations.
- **Cost efficiency:** Altering recovery sequences can help you to reduce costs. For instance, authenticating the user with an OTP stops most criminals before they reach identity verification. Our service can tell if they are using a spoofed device, blacklisted phone number or a fake or stolen number, for example.

Removes complexity and costs: With a unified platform, there's no need to cross-correlate data and standardize risk scores from multi-vendor solutions. Our centrally-managed platform provides native identity verification and a complete set of authentication methods, including best-in-class passwordless MFA and passkeys with added security. A unified user store provides visibility of each users' devices, authenticators, risk scores and applications via one console — providing a single source of truth with graphical displays of real-time data, attack patterns and trends.

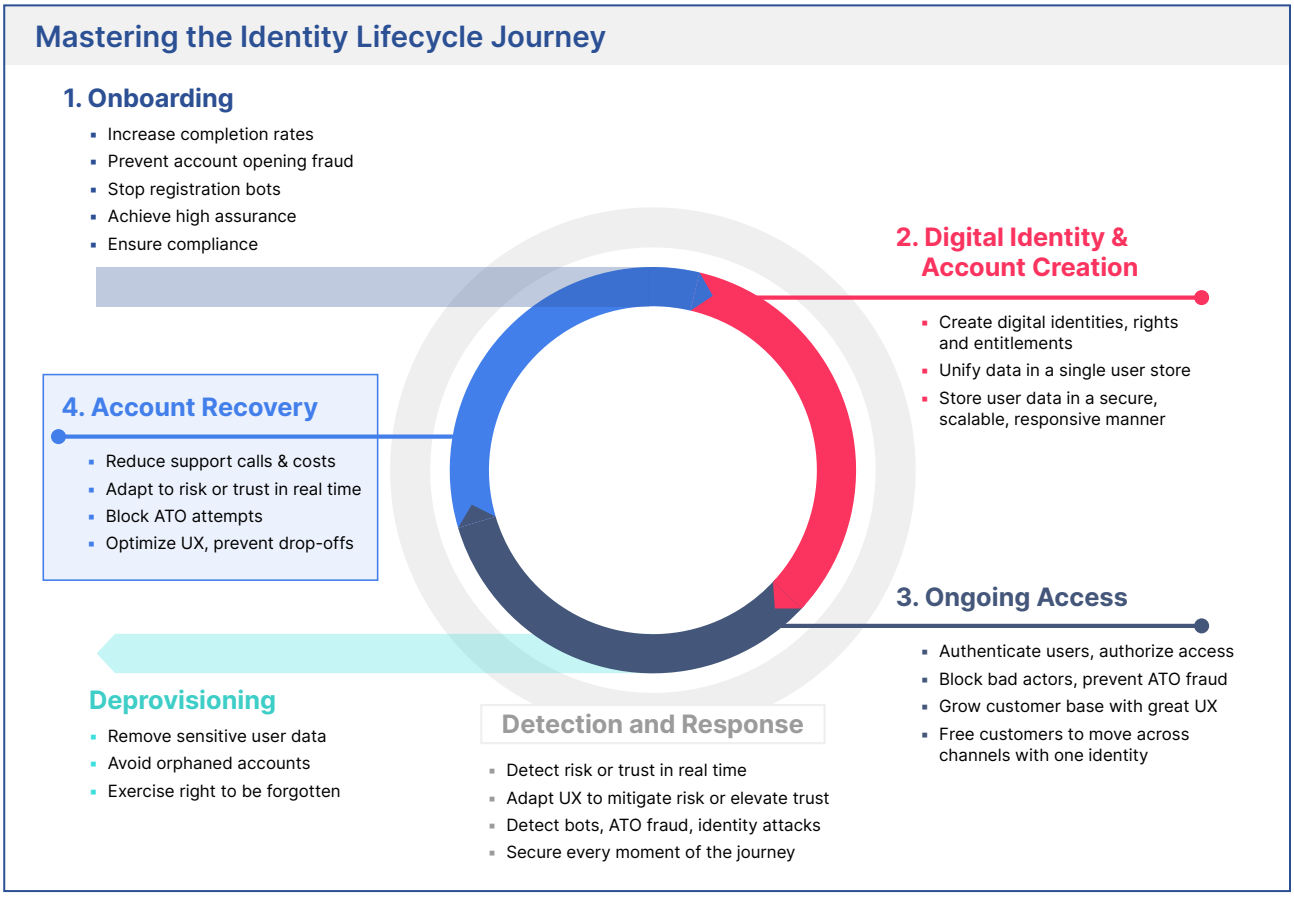
Better UX: Customers can choose their preferred account recovery methods and are assisted in switching to phishing-resistant credentials when they're ready. Passive security measures, such as behavioral biometrics and device fingerprinting, increase the LOA without interrupting the customer experience. Journey-time orchestration adapts the login experience at runtime, removing friction for trusted customers. You'll retain more customers, lower support costs and increase revenue.

Frictionless and secure account recovery

Transmit Security delivers a complete use case solution to solve all of the complex, multi-faceted account recovery challenges out of the box. Our unified platform prevents fraudsters from exploiting weaknesses in the account recovery process — while minimizing the demands on the customer to prove their identity.

Our holistic identity-security platform provides the full range of authentication methods, including true passwordless authentication and passkey security, plus real-time fraud detection, native identity verification and the leading journey-time orchestration — all powered by ML, AI and GenAI to meet the strictest security and UX requirements.

With secure and simple account recovery, companies are improving the customer experience and reducing support costs while cutting fraud losses and boosting revenue.



With a layered, **plug-and-play solution purpose-built for use cases**, you'll gain full platform synergies to quickly adapt to risk, trust and evolving threats. Cloud-native capabilities work in concert to deliver the agility, simplicity, speed and accuracy you need — along with the cost-efficiency and limitless scale to keep millions of customers happy and loyal.

Discover how Transmit Security stops fraud and rewards customers with easy and secure account recovery, so they can break free and access all that your business offers.