Account Takeover (ATO) fraud is lucrative, low-risk, and a growing threat for financial institutions. Data breaches, stolen identities, and fraud scams are behind rising ATO attacks, with losses averaging $12,000 from over 24 million US households*. Traditional ATO solutions can't stop attacks before the transaction stage. It's time to change the game; prevention needs to happen proactively, not reactively, without adding customer friction. Silently detect user anomalies and protect customers from credential theft, impersonation, and manipulation attacks across every interaction.

Detect and prevent ATO attacks.

Stop ATO attacks in real-time
Prevent ATO attacks at every online interaction by collecting and analyzing customer biometric and interaction behavior, network, and device data – their BionicID™ in real-time. Feedzai’s Active Defense proactively stops malware, phishing, and Remote Access Trojans before they can cause harm.

Ensure users are trustworthy
Our Know Your User approach continually and silently asks, “are you really you?” utilizing a user’s BionicID™ to identify legitimate customers, stop fraud before it happens, and improve the customer experience by eliminating step-up authentications.

Improve transaction decisioning
User BionicID™ data and analysis is pre-integrated with Feedzai’s Transaction Fraud for Banks and can also be used by other transaction monitoring, or SIEM solutions to provide user interaction data and analysis for every session to improve transaction decisioning accuracy.

---

1 Security.org, Account Takeover 2021 Annual Report: Prevalence, Awareness and Prevention, February 2021
Key Features

**Behavioral biometrics**
Customer BionicIDs are based on the analysis of hundreds of online behavioral parameters including devices, account behavior, geolocation, and more.

**Hybrid AI**
Customer BionicIDs are created and maintained by hybrid AI technology that enables you to really know your user and protect them from login to logout.

**Silent customer experiences**
Prevent customer friction by silently authenticating users at every interaction without the need for friction-inducing verification methods.

**Active defense**
**Manipulation attacks**
Stop ID-stealing malware or phishing attacks by preventing users from being manipulated into compromising their credentials.

**Impersonation attacks**
Protect customers from Remote Access Trojan session hijacking malware automatically via step-up authentication or automatic session logoff actions.

**Real-time session data and analysis**
Customer session and threat data can readily be integrated into transaction management, fraud hub, or SIEM systems to improve transaction decisions.

Awards and Recognition

*Feedzai placed #15 on the Forbes list of most promising AI companies.*

*Feedzai was named best-in-class fraud and AML machine learning platform vendor.*

*Feedzai was bestowed Top 21 RegTech Innovation Award.*

Are you ready to start proactively protecting your customers?

Request a Demo