feedzai | Solution Guide

Using Digital Trust to Stop Impersonation and Manipulation Attacks

#ProtectYourCustomers

feedzai.com

Contents

Both **impersonation** and **manipulation attacks** are the gateways for bad actors to commit account takeover (ATO) attacks. ATO attacks can inflict significant financial damage. Total consumer losses in the US related to identity fraud losses – including ATO attacks – and other identity fraud rose to $52 billion (USD) in 2021. Losses from ATO attacks increased by 90%.

Impersonation Attacks start with stolen credentials, which are often obtained through tactics like phishing, malware, or data breaches. Fraudsters use a legitimate customer's compromised credentials - such as their email addresses, passwords, usernames, or phone numbers - to pose as the customer and access their accounts.

In Manipulation Attacks, fraudsters utilize legitimate remote access software or trick victims into executing a form of malware (known as a **Remote Access Trojan**) to hijack a device or online banking session. This form of attack is easier to execute, yet more difficult to detect because it bypasses traditional account security, allowing a bad actor to temporarily control a victim's account.

US Consumer Losses in 2021

$52Bn

total losses related to identity fraud losses

90%

increase in losses from ATO attacks

How Feedzai Uses BionicIDs™ to Stop Impersonation and Manipulation Attacks

Feedzai analyzes thousands of users, network, and system parameters collected during every online interaction or operation to safeguard users from impersonation and manipulation attacks.

Feedzai's Digital Trust first collects thousands of non-PII parameters starting with behavioral biometrics - how a user physically interacts with their device. Secondly, behavioral analytics is layered in for a deeper understanding of when, where, and what the user accesses across all digital channels. Thirdly, device and network data is analyzed to uncover any suspicious access to a protected website or mobile application server. These are the fundamental building blocks of a BionicID™ - Feedzai's unique digital profile of an individual customer.

The customer's behavioral biometric data is processed in the cloud using hybrid AI models including Deep Learning to create a BionicID™ for all users, legitimate or bad actors at sign-up. From that point, it is continually updated and analyzed at every interaction, and a holistic risk score is calculated for each customer.

In today's post-breach world, stolen credentials are readily available for bad actors to use to impersonate legitimate users. Feedzai prevents malware or phishing attacks from stealing user credentials in the first place.

Feedzai's Digital Trust also allows banks to determine the appropriate actions to take when malware attacks or phishing attacks are detected on user devices - and immediately, automatically, and silently protect those users as well as alert the bank's fraud teams.

> **A BionicID™ for all users is continually updated and analyzed at every interaction, and a holistic risk score is calculated for each customer.**

Stolen credential attacks require a different approach to stop since they are executed by credential stuffing bots and manually by humans. These kinds of attacks are detected, and account takeovers are prevented by BionicID™ analysis.

This form of attack is easier to execute because it bypasses traditional account security, allowing a bad actor to temporarily control a victim's account. Feedzai's BionicID™ analysis can detect and defeat both attack types, stopping attempted session takeovers before funds are moved - protecting users and notifying the bank.

Depending on the risk, the system silently allows user access or stops bad actors. The bank has control over risk score thresholds, can configure when to be alerted, and can also automate workflows so that appropriate action can be taken. For example, if an impersonation or manipulation attack is detected, Feedzai provides banks with two flexible response paths.

1. **Protect users at the point of attack immediately.**
2. **Simultaneously alert the bank's fraud teams of the attack and execute a follow-up response – ranging from sending user notifications, stepping up authentication, terminating a session, or locking the account – stopping fraud before it happens.**

What is BionicID™ Analysis Best Suited For?

BionicID™ is most commonly used by financial institutions for anti-fraud or user verification applications, to stop online fraud.

For example, in online behavioral biometrics in banking applications, BionicID™ analysis can provide effective fraud protection against manipulation or impersonation-based attacks such as account takeover (ATO) fraud, as well as malware-based ones such as Remote Access Trojans (RATs).

Besides online banking access, BionicID™ analysis can also be applied to other use cases such as detecting New Account Fraud, Card Not Present, or when 3D Secure verifications are required.

Does BionicID™ Data Collection or Analysis Impact the User Experience?

BionicID™ data collection is entirely transparent for end-users, and the data analysis is invisible without requiring users to take any extra steps. Furthermore, it works in the background and provides passive biometric verification to confirm the person behind the online session is always the genuine user.

When a BionicID™ anomaly is detected, the bank has the option of layering in additional authentication (multi-factor authentication). Similarly, during a 3D Secure stepped-up verification, users may be required to take additional steps to verify their identity.

Deep learning algorithms continuously evaluate the incoming flood of behavioral biometric data on the financial institution's side. This evaluation will result in a seamless and secure user experience or, in the case of anomalous activity, trigger an automated response to stop an attack and follow-up alert to notify the bank of the attack and the actions taken to prevent it.

> **This evaluation will result in a seamless and secure user experience or, in the case of anomalous activity, trigger an automated response to stop an attack.**

Does BionicID™ Data Collection/ Analysis Comply with SCA/PSD2?

BionicID™ data collection and analysis comply with Strong Customer Authentication (SCA) requirements. They can be used as a component of multi-factor authentication as required by the EU's Second Payments Services Directive (PSD2).

Strong Customer Authentication is required through PSD2 every time someone attempts to pay online or access their online banking services. The authentication must be carried out by the Payment Service Provider (PSP).

It must occur through at least two different factors that satisfy two of three categories:

Possession (device)	**Knowledge** (password or PIN)	**Inherence** (something the user has - physical biometrics such as a fingerprint or behavioral biometric security)

When combined with deep learning technology, behavioral biometrics for human identification can authenticate a user invisibly and throughout their entire online banking session, meaning a factor of authentication (in this case inherence) under SCA is fulfilled with no user action required.

Additionally, the use of BionicIDs™ is also compliant with other international cybersecurity standards and regulations set forth by NIST 800-171, ISO 27001, HIPAA, FINRA, and FISMA.

> **Behavioral biometrics for human identification can authenticate a user invisibly and throughout their entire online banking session.**

Does BionicID™ Data Collection/Analysis (Behavioral Biometric Digital Identity) Comply with GDPR?

BionicID™ data collection and analysis complies with the European Union's General Data Privacy Regulation (GDPR). GDPR requires organizations to demonstrate that the people they store personal data on have given their explicit consent to data processing and can ask for their data to be erased. Since banks handle extremely sensitive personal information, users demand the highest levels of data protection from them.

The most basic operating principle of behavioral biometric analysis is that personal information alone can no longer be a trusted source of authentication. For example, a user's password, email, and mother's maiden name all constitute data that can be easily stolen, leaked, and traded. In comparison, behavioral biometric data is invisible and irreplicable.

Feedzai undertakes non-intrusive checks during a customer's online session without storing confidential or private user data while providing banks with the guarantee that users are who they say they are.

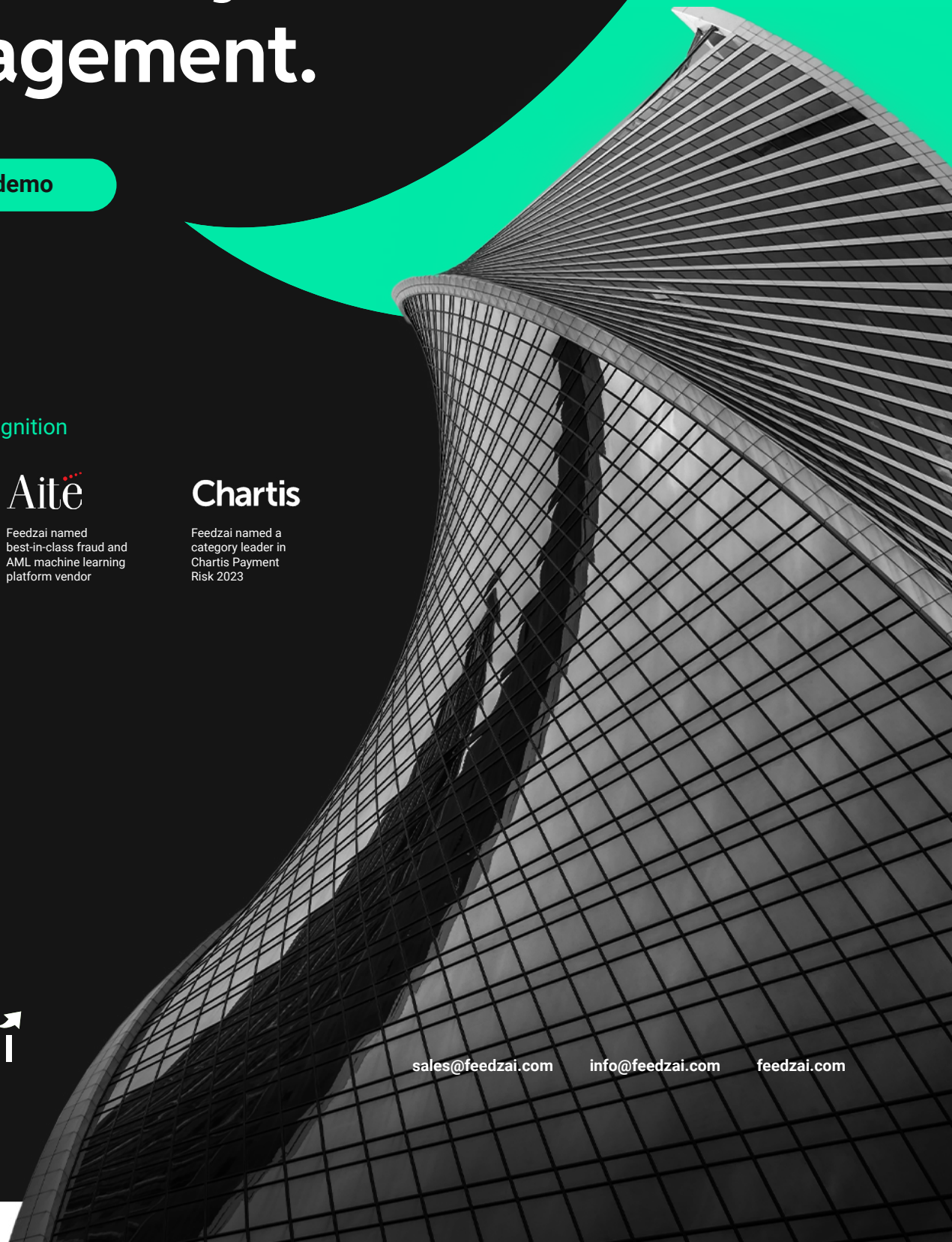
See for yourself how Feedzai's Digital Trust works. Get in touch or request a demo and we'll get you connected with one of our experts!

> **Feedzai undertakes non-intrusive checks during a customer's online session without storing confidential or private user data.**

The world's first RiskOps platform

Transform your risk management.

Request a demo



Awards and Recognition

Quadrant Knowledge Solutions

Feedzai named a leader in SPARK Matrix AML.

Aité

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

Chartis

Feedzai named a category leader in Chartis Payment Risk 2023

feedzai

sales@feedzai.com info@feedzai.com feedzai.com