

Plugging the gaps and vulnerabilities in booking travel: From Agentic AI to call centres – minimising the risks



Niall Whelan
Head of Asia
Darwinium

Loyalty Now And Then

2016

Loyalty contained to primary brand and limited partners

Limited redemption surface, easy to observe & risk

2026

Loyalty shared across multiple brands and partners

Multiple redemption journeys, difficult to get a unified view of risk

2036?

What new challenges will AI bring to loyalty schemes?

AI Fraud Has a Favorite Industry: It's Yours

Travel and aviation are bearing a disproportionate share of the AI impact

17% of travel and airline leaders say AI-assisted fraud has increased dramatically in the last year

2.5x cross-industry average

Now Boarding: The Agentic Traveler

Airlines and OTAs are expecting non-human traffic across the customer journey

33%

Estimate that between a quarter and a half of their traffic is non-human today.

10pp above average.

61%

Expect non-human traffic to go up dramatically or significantly over next 12 months.

8pp above average.

63%

Expect agents to perform account actions such as booking changes / cancellations.

8pp above average.

The Agentic Paradox

The same technology enabling good customers is equipping fraudsters

Trusted customers will use agents to:

- Make travel decisions
- Compare products / prices
- Make payments

Fraudsters will manipulate agents to:

- Find booking weak spots
- Bypass application and login protocols
- Create realistic deepfake, scam and phishing attempts

46%

of airlines & OTAs say they can't distinguish good / bad agentic traffic

56%

say they can't authenticate the agent's intent

Loyalty - The New Frontier for Fraud

\$3.1Bn

of redeemed loyalty points are fraudulent.

Loyalty Security Alliance.

72%

of loyalty programs experience fraud

Brandmovers

45%

of loyalty accounts are inactive

Brandmovers

52%

of loyalty attacks are Account Take Over

Brandmovers

Q: What other industry has a large value store been constantly targeted by new and innovative fraud?

A: Banking

Introducing M.I.L.E.S.

Five patterns behind airline loyalty fraud - and the bank playbook that beats them

M	I	L	E	S
Multi-Accounting	Impersonation	Lure	Extraction	Signals
<i>Fake accounts, mass-created</i>	<i>Stolen logins, hijacked accounts</i>	<i>Social engineering scams</i>	<i>Points laundered & resold</i>	<i>The bank's defense playbook</i>



Multi Account Creation

Bots and phone farms mass-produce fake loyalty accounts

Opening a loyalty account takes only an email or phone - no KYC required, unlike a bank

Phone farms: hundreds of devices acting in concert to sign up via airline apps and sites

Fraud bots increasingly mimic legitimate agentic booking assistants - telling them apart is now the hard part

SIGNALS BANKS LOOK FOR

Lack of natural device movement

Constant charging, consistent light exposure

Unusual app counts, typing or touch patterns

VPN use, suspicious networks, direct API calls



Impersonation And Account Takeover

Stolen credentials meet accounts that skip strong authentication

MFA is standard at banks but optional at most airlines, which prioritize a frictionless experience

Credential stuffing tests usernames and passwords leaked in prior breaches, at scale

Persistent device fingerprinting flags one device targeting many accounts

BANKS DETECT INTENT, NOT ANOMOLY

“A legitimate user checks their balance. A criminal moves straight to changing contact details and redeeming points.”

Trusted devices earn a white-glove, low-friction journey.



Lure Of Social Engineering Scams

As digital defenses improve, criminals recruit the victim to do the work

A call, text, or email warns customer of an “urgent security risk” on the account

Upon contact, the victim is talked into screen-sharing or granting remote access “to fix it”

As they’re using their own device and credentials, the activity can appear legitimate

BANKS SHUT DOWN SESSION WHEN THEY SEE

An active call

Screen sharing

Remote-access tools

Unusual transfer behavior

User hesitation



Extraction : Ghost Brokering

The payoff: fraudulently acquired inventory sold to unsuspecting customers

Fraudster drains or transfers the stolen points balance to a central account

Resells travel inventory through unofficial channels

Combines multiple techniques to acquire airline inventory fraudulently

BANKS LOOK FOR MULES

Mule accounts are purchased, compromised or synthetically created

Used for the explicit purpose of receiving stolen points

Aggregation and large TX are tells



Signals Across the Journey

The bank playbook: multiple layers of intelligence, watching every step

Network intelligence - VPNs, proxy use, suspicious IPs and direct API traffic

Device intelligence - forensics on configuration, familiarity, and velocity

Behavioral biometrics - typing, touch, and navigation patterns unique to each user

THE AGENTIC IMPACT

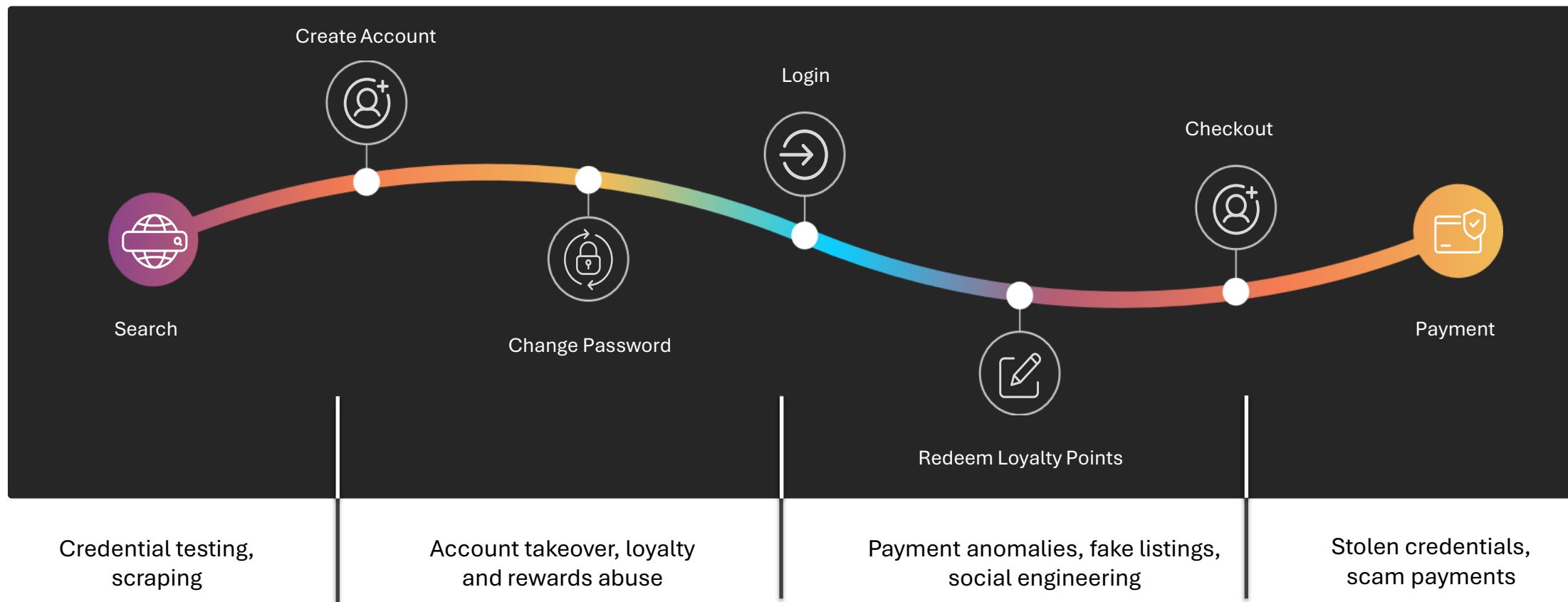
Journey-wide signals are the only way to differentiate a trusted agent from a criminal one

The same intelligence that stops loyalty fraud today future-proofs against agentic threats tomorrow



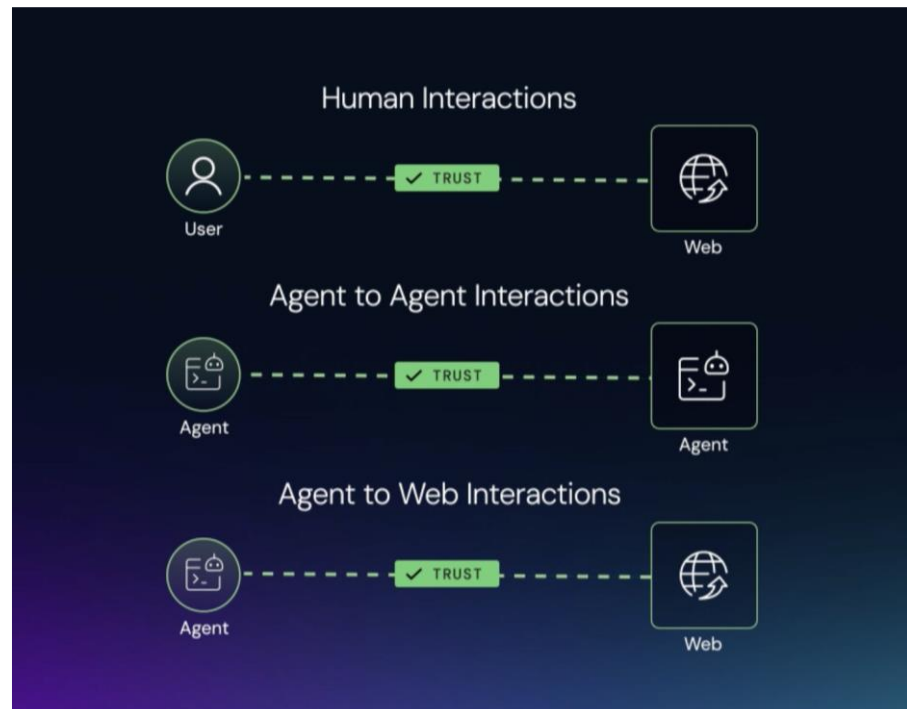
Shift The Mindset

Understand intent across journeys, not transactions. Remove the blind spots



See Users And Their Agents

Embrace agentic traffic by classifying agent behavior



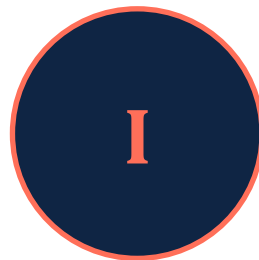
User 1	Agent 1	User 2	Agent 2
✓ DEVICE	✓ DEVICE	✓ DEVICE	! DEVICE
✓ IDENTITY	✓ IDENTITY	✓ IDENTITY	✓ IDENTITY
✓ LOCATION	! LOCATION	✗ LOCATION	✗ LOCATION
✓ NETWORK	✓ NETWORK	! NETWORK	✗ NETWORK
✓ BEHAVIOR	✓ BEHAVIOR	✗ BEHAVIOR	✗ BEHAVIOR
✓ JOURNEY	✓ JOURNEY	! JOURNEY	✗ JOURNEY

Think Like A Bank

Banks have already built the playbook - airlines just need to fly it.



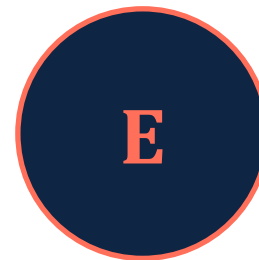
**Multi-
Accounts**



Impersonation



Lure



Extraction



Signals

The fraud is new. The playbook isn't.

Questions