imper.ai

CASE STUDY

How a national retailer uses imper.ai to stop Scattered Spider vishing at the help desk.

INDUSTRY	WORKFORCE	ITSM	RESULT
Retail	**15,000+**	**ServiceNow**	**Recovery blocked. Account intact.**

Challenge

The organization operates a national retail network with over 15,000 employees across store locations and distribution centers. Identity infrastructure runs on Okta, Microsoft Entra ID, and ServiceNow. The help desk is split between in-house and outsourced agents, with outsourced staff measured on resolution speed and carrying no institutional familiarity with individual employees. Account recovery for employees locked out of their MFA device cannot satisfy standard authentication and is forced into a manual verification workflow where agent judgment becomes the primary control.

A financially motivated threat actor operating consistent with **UNC3944 and Scattered Spider** TTPs targeted a mid-level IT administrator with elevated access to identity infrastructure. The attacker conducted reconnaissance using LinkedIn and public-facing directories, then called the help desk with a deliberate pretext: a lost authenticator. Scattered Spider exploits the outsourced help desk structurally. **The vulnerability is not undertrained agents.** It is a process that gives agents no reliable identity verification mechanism when standard authentication cannot apply.

> **We had invested significantly in our IAM stack. What we had not solved was what happens when someone calls in and our standard authentication controls cannot apply. That is exactly the gap that was targeted, and exactly what imper.ai closed.**

CISO, Leading National Retailer

Risk & Impact

#1
cloud initial access vector in 2025
Mandiant M-Trends 2026

up to 50%
of help desk calls are password resets or account recovery
Gartner

£300M
lost operating profit at M&S following Scattered Spider help desk attack
M&S annual results, May 2025

Solution

When the recovery request entered the ServiceNow workflow, imper.ai's Impersonation Detection Engine began analyzing signals at two layers. At the inbound call, the originating phone number was flagged against VoIP carrier reputation. When the help desk agent sent the verification link to the caller, the link opened in a browser running inside a virtual machine, with the session originating from a residential proxy. imper.ai detected the non-native device environment from device and session signals — not by recognizing a specific piece of software, but by identifying that the session was not running on a real endpoint.

How it works

For help desk vishing, two detection layers run in sequence and both must clear before recovery proceeds. The Impersonation Detection Engine analyzes device, network, and infrastructure signals across every account recovery and credential event, surfacing attacker-controlled environments such as anonymizing proxies, remote access tooling, and geolocation anomalies. AI-Driven Contextual Verification then confirms the caller is the actual account holder through dynamic, role-based questions grounded in the employee real work context. An attacker with the employee full personal profile cannot answer what the employee did yesterday.

Outcome

No credentials modified

The recovery workflow was terminated before any password was reset or MFA device re-enrolled. The attacker did not obtain an authenticated session.

Policy-enforced outcome

In-house and outsourced agents had no discretion over whether the request could proceed. The result did not depend on who answered the call.

Downstream systems protected

Okta, Microsoft Entra ID, and Active Directory remained secure. A successful re-enrollment would have provided authenticated access across all three.

Embedded within existing workflows

Both detection layers are enforced at the application level inside ServiceNow, Okta, and Microsoft Entra ID. The agent receives a verification signal and has no discretion over whether the request proceeds. Help desk process does not change. imper.ai surfaces the risk score and contextual verification result inside the existing ticket.

imper.ai

imper.ai is a Workforce Identity Verification platform built to detect and stop impersonation attacks across the employee lifecycle. As MFA adoption has increased, threat actors have shifted to the workforce workflows surrounding identity, help desk recovery, MFA re-enrollment, credential issuance, and hiring. imper.ai addresses that gap through real-time infrastructure-layer signal analysis and AI-Driven Contextual Verification, integrated into the platforms security and IT teams already operate.

Get a demo!