Mitek

Secure every link: your guide to omnichannel fraud defense

AI-empowered fraudsters are exploiting the weakest link in your defenses — your employees. From in-store retail and telecom to branch banking, here's how they're doing it:

Telecommunications fraud:
Fraudsters visit retail locations to obtain phones and service agreements using fake IDs or hijacked account information.

Banking fraud at branches:
Fraudsters use counterfeit or stolen documents to open bank accounts, apply for loans, or make withdrawals from another person's account.

Car dealership fraud:
Fraudsters use fake identities or financial information to test drive, lease or purchase, often with no intention of making payments or returning the car.

Healthcare fraud:
Fraudsters use another person's insurance information to receive medical care or prescription medications.

Rental and real estate fraud:
Fraudsters pose as renters or buyers using false information to secure leases or property purchases.

Retail store credit fraud:
Fraudsters present fake IDs to apply for instant credit or make large purchases at retail stores.

Identity fraud is a growing threat

72% An astounding 72% of banks and financial institutions said their organization faced cases of synthetic identities when onboarding new clients.[1]

12% Telecommunications fraud, including practices like SIM swapping, increased by 12% in 2023, resulting in an estimated $38.95 billion in losses.[2]

$1.8B Auto lenders experienced a significant increase in potential losses, reaching $1.8 billion, up from $1.3 billion in the same period the previous year.[3]

Humans are fallible

Today's fake IDs or falsified documents are almost impossible for customer-facing teams to detect without the support of AI-powered defenses.

Knowledge gaps:
Employees often miss signs of identity fraud due to insufficient training on the latest forgery techniques and how to overcome bias when verifying a person's identity.

Detection challenges:
Modern fake IDs feature high quality holograms, watermarks, and other counterfeit details that easily fool the human eye, especially in hectic or high-pressure situations.

Human vulnerabilities:
Fraudsters are adept at exploiting human emotions and biases, using urgency, confusion, or social engineering tactics to effectively bypass established security protocols.

An omnichannel strategy is the best defense

Take action to block fraud consistently everywhere you interact with customers – online and in the real world. It's the best way to maintain a robust defense against opportunity-seeking fraudsters.

Integrate digital verification tools:
Provide employees with access to AI-powered technologies that can quickly and accurately verify identities including facial and voice biometrics, liveness detection, ID document validation, database checks, geolocation, velocity scans, and digital footprint analysis.

Cultivate trust:
Help employees understand that customer trust is as valued as sales. Integrate fraud prevention metrics into employee performance evaluations and reward employees for diligent verification practices and successful fraud prevention.

Protect the good customer experience:
Strike the right balance between customer convenience and business risk. Adopt solutions that can perform additional checks dynamically and only if warranted based on actual risk factors.

Stay ahead of in-person fraud

Empowered and opportunistic fraudsters are walking through your front door. Are you prepared? Protect your business with an omnichannel fraud defense. Get started with our free guide and planning blueprint.

Get the Guide

Sources:
1. 2024 AI, Fraud, and Financial Crime Survey, Biocatch, 2023.
2. Communications Fraud Control Association, November 13, 2023.
3. Synthetic identity fraud on rise, ABA Banking Journal, August 24, 2023.