OMNARETH

SOLUTION BRIEF

Identity Verification Fraud Prevention

Verify the person. Not the forgery.

The challenge

A ring opens hundreds of onboardings under invented names. Each one fails or passes on its own; the ring only shows across onboardings.

The solution

Synthetic identity rings open accounts with forged documents, deepfakes injected through virtual cameras, photos held up for the liveness check and stolen documents. Omnareth checks every document and selfie result before the account opens, and recognizes the ring's device, a reused document or a reused face across onboardings.

14
reference rules for identity verification

75 ms
median fraud-checked, audited decision, lab test

8/8
reference scenario decisions correct and verified on chain

How it fits

ELEMENT	IN THIS SOLUTION	WHAT IT COVERS
The record	The onboarding	The details the applicant declared and your policy: accepted documents, the lowest face match you accept, attempts allowed.
The events	Document and selfie checks	A document must be accepted, current, untampered and match the declared details; a selfie must be live, real and match the document.
The memory	One device, many applicants	The ring's device is held responsible, never the person whose document was stolen.

> **Evidence for auditors and regulators**
>
> Every decision stores the record, the request and the exact rules evaluated, with what was known about everyone involved, under a SHA-256 integrity hash anchored on the Omnareth chain. Edits, even covered-up ones, fail verification.

Next step: run the scenario with your team (`examples/identity-verification/demo.sh`, one command, every record verified), then scope a 90-day shadow-mode pilot. See the Pilot Program Guide.

© 2026 Habify Labs, Inc. All Rights Reserved. · Omnareth

What it stops

RULE	WHAT OMNARETH CHECKS	DECISION
Details Do Not Match	The date of birth on the document must match the one declared.	DENY
Document Expired	An expired document cannot prove identity.	DENY
Document Not Accepted	Only document types the business accepts may be used.	DENY
Document Tampered	Deny a document whose security features or data show tampering.	DENY
Onboarding Not Open	Checks run only on open onboardings.	DENY
Face Does Not Match	The selfie must match the document photo above the business's threshold.	DENY
Injected Camera Feed	A selfie streamed from a virtual camera or emulator may be a deepfake.	DENY
Liveness Failed	A selfie must come from a live person, not a photo, screen or mask.	DENY
Too Many Attempts	Flag a selfie after more attempts than the policy allows.	FLAG
Device Across Onboardings	Flag a device implicated in denied checks on 2+ other onboardings in 24 hours.	FLAG
Document or Face Reused	A document or face belongs to one person; seen on another onboarding, it may be stolen or synthetic.	FLAG
Repeat Offender	Flag events involving an identity implicated in two or more denied events in the last 30 days.	FLAG
Blocked Identity	Identities blocked on the fraud watchlist may not take part in any onboarding event.	DENY
Watched Identity	Identities under watch may proceed only with a flag for review.	FLAG

The reference scenario

#	EVENT	DECISION	FRAUD CASES
1	Genuine applicant scans a passport	ALLOW	
2	Tampered driving licence from the ring's emulator	DENY	
3	Deepfake selfie through a virtual camera, same emulator	DENY	Repeat offender; device watched
4	Photo held up to the camera, same emulator	DENY	One device across three onboardings: case opened
5	Genuine selfie passes on the fourth try	FLAG	
6	The ring presents the genuine applicant's stolen passport	DENY	One passport on two onboardings: case opened
–	Analyst confirms the device case	-	Emulator blocked everywhere
7	After a reviewer lowers the face-match threshold, a 41% match retries	DENY	
8	Genuine applicant scans a national ID card	ALLOW	

© 2026 Habify Labs, Inc. All Rights Reserved. · Omnareth