DEFENCE CHECKLIST

Synthetic identity fraud defence checklist

Zyphe

Run the toolkit. None of these, on its own, proves a real, unique human is applying.

CONTROL	WHAT IT CATCHES	WHAT IT DOES NOT CATCH
SSN to name to DOB consistency checks	✓ Crude mismatches and recycled fragments	✗ A clean, internally consistent fullz
eCBSV Social Security number verification	✓ A name, DOB and SSN that fail SSA records	✗ A real SSN paired with fabricated details
Device and velocity signals	✓ Bulk applications and burst patterns	✗ A patient fraudster cultivating one identity
Consortium and shared-data signals	✓ Identities already flagged across members	✗ A brand-new synthetic with no footprint
Behavioural analytics	✓ Bot-like or anomalous session behaviour	✗ A careful human operator behaving normally
Perpetual or ongoing KYC	✓ Risk that emerges after onboarding	✗ Whether the applicant is one real person
Verify without centrally storing PII	✓ Removes the honeypot that supplies fullz	✗ Not a fraud score; a structural change

The structural fix: verify, do not warehouse.

Zyphe shards verified data across 60,000+ nodes under a 29-of-100 threshold scheme, so no single node holds a complete record. The customer holds the key and there is no master key. A reusable KYC passport means fewer copies of raw data exist to steal.

zyphe.com · General information, not legal advice