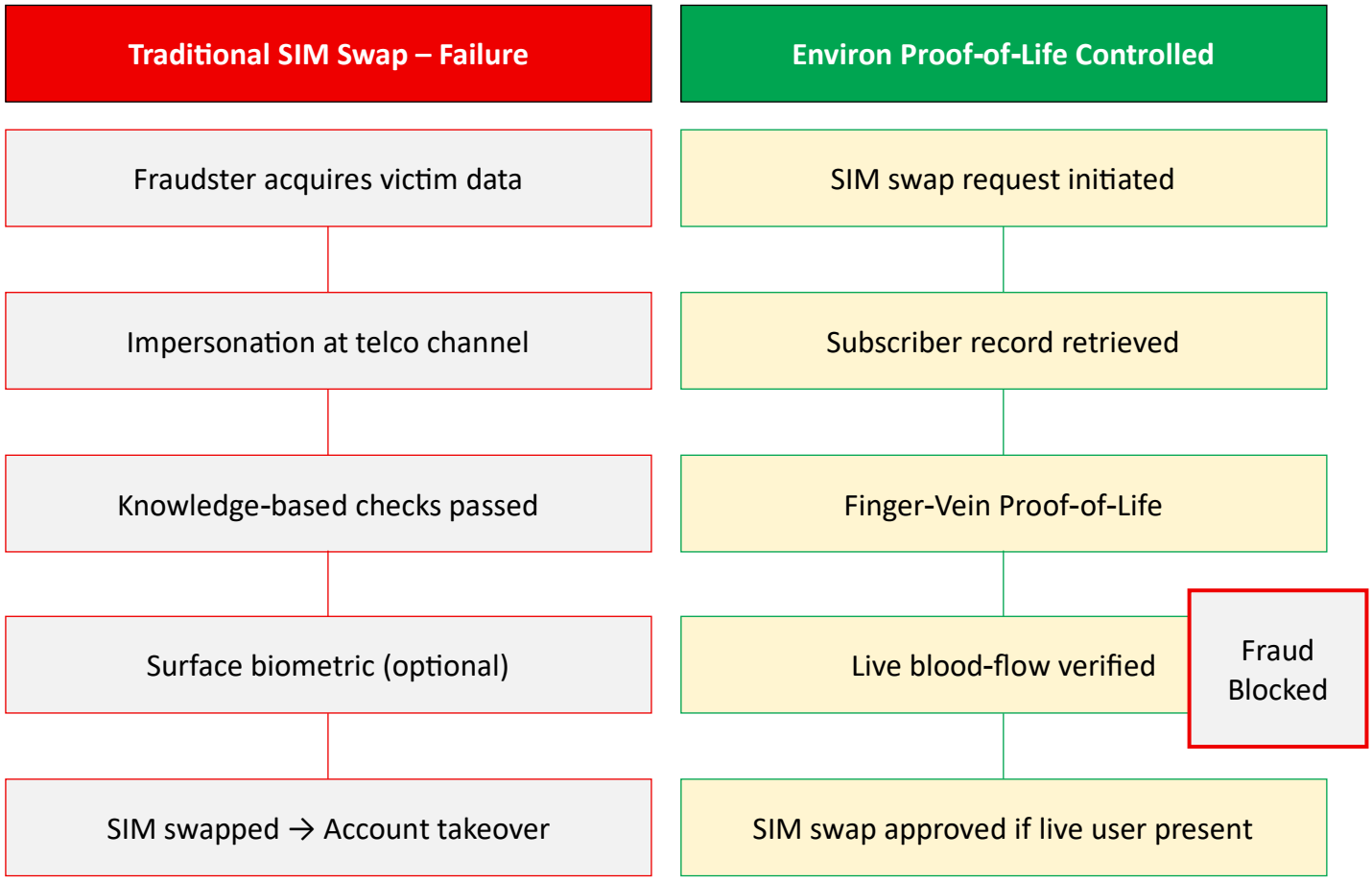
ENVIRON - SIM Swap & bank Fraud Incident Flow

A side-by-side comparison of traditional SIM swap failure versus Environ Finger-Vein Proof-of-Life control.

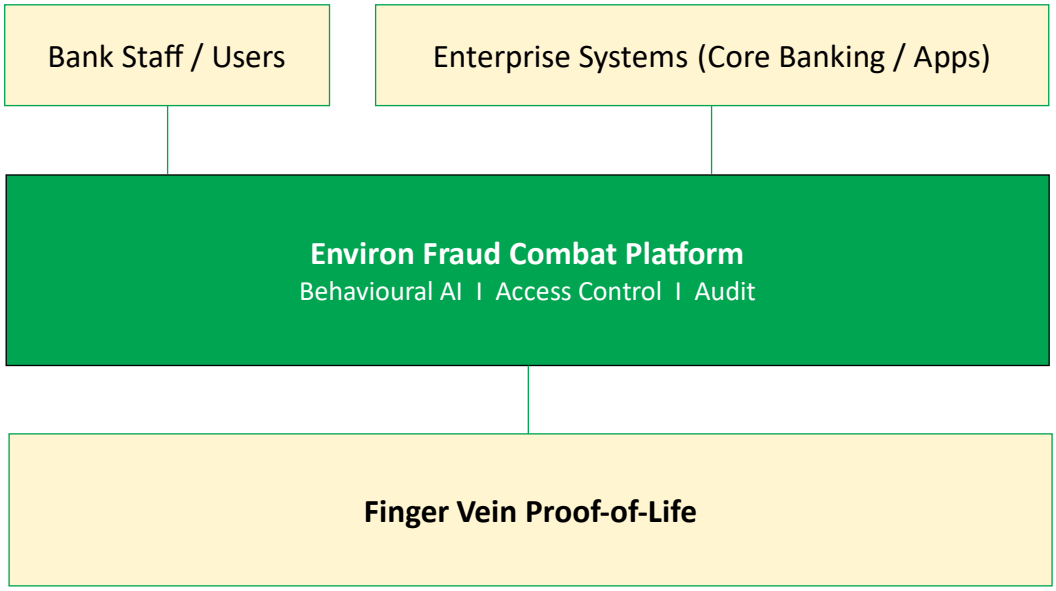


Control	Traditional SIM Swap	Environ Proof-of-Life
Identity check	PIN / PII / surface biometrics	Sub-dermal finger-vein
Spoof resistance	Low	Very high (live blood-flow)
Insider abuse risk	High	Strongly mitigated
Inclusion (worn fingerprints)	Low	High
Fraud outcome	Account takeover	Attack blocked

Environ Finger-Vein Proof-of-Life converts SIM swap from a weak administrative process into a high-assurance, inclusive identity control suitable for National ID, telecoms, and banking.

High-Level Architecture Overview

This architecture illustrates how Environ integrates behavioural intelligence, access control, and Finger Vein Proof-of-Life into core banking and enterprise systems.



Nigeria-Specific Fraud Risk Context

Nigeria represents one of the fastest-growing digital financial markets globally, while also experiencing rising levels of fraud driven by identity compromise, insider abuse and social engineering.

Risk Area	Indicative Impact
Electronic & Digital Fraud Losses	1 trillion+ estimated annual impact
Insider & Privileged Abuse	Among the hardest to detect and prosecute
Account Takeover & Social Engineering	Rapidly increasing with AI-enabled scams
Weak Authentication Controls	Primary enabler of fraud escalation

Regulators and financial institutions increasingly require Proof-of-Life controls, insider visibility and audit-grade accountability to protect customers and maintain trust.