Rebuilding Cross-Border Trust in Voice Communications

A critical imperative for protecting consumers and restoring confidence in international voice networks

The Global Crisis: Voice Fraud Knows No Borders

Noida, India
July 2025

Raided call center posing as Microsoft tech support defrauded UK residents of more than £390,000. Required 18-month investigation across three countries to shut down.

Montréal, Canada

“Grandparent scam" ring impersonated distressed relatives, convincing elderly Americans to send emergency cash. Over $21 million stolen across hundreds of cases.

Myanmar Border Zones

Entire scam compounds established where thousands of trafficked workers are forced to run call-based fraud operations targeting victims worldwide.

The Staggering Human and Economic Toll

$37B

Annual global cost

UN estimates for cross-border telecommunications scams in 2023 alone

18

Investigation months

Average time required for cross-border fraud enforcement actions

1000s

Trafficked workers

Forced to operate scam call centers in Southeast Asian compounds

All of these attacks share one critical vulnerability: they exploit the breakdown in identity verification when calls cross international borders. When networks cannot authenticate who is on the line, criminals can impersonate anyone—tech support agents, government officials, or family members.

The result: Lost money, shattered confidence, and a global public that no longer trusts their phone.

To rebuild that trust, we must start with authentication

Authentication is the foundational pillar of identity in all communication systems

What Authentication Delivers

Authentication verifies that a communication originates from the person or organization it claims to represent. It is the digital equivalent of an ID check at a secure facility.

Consumer Protection

Shielded from impersonation attacks and sophisticated scam operations

Business Confidence

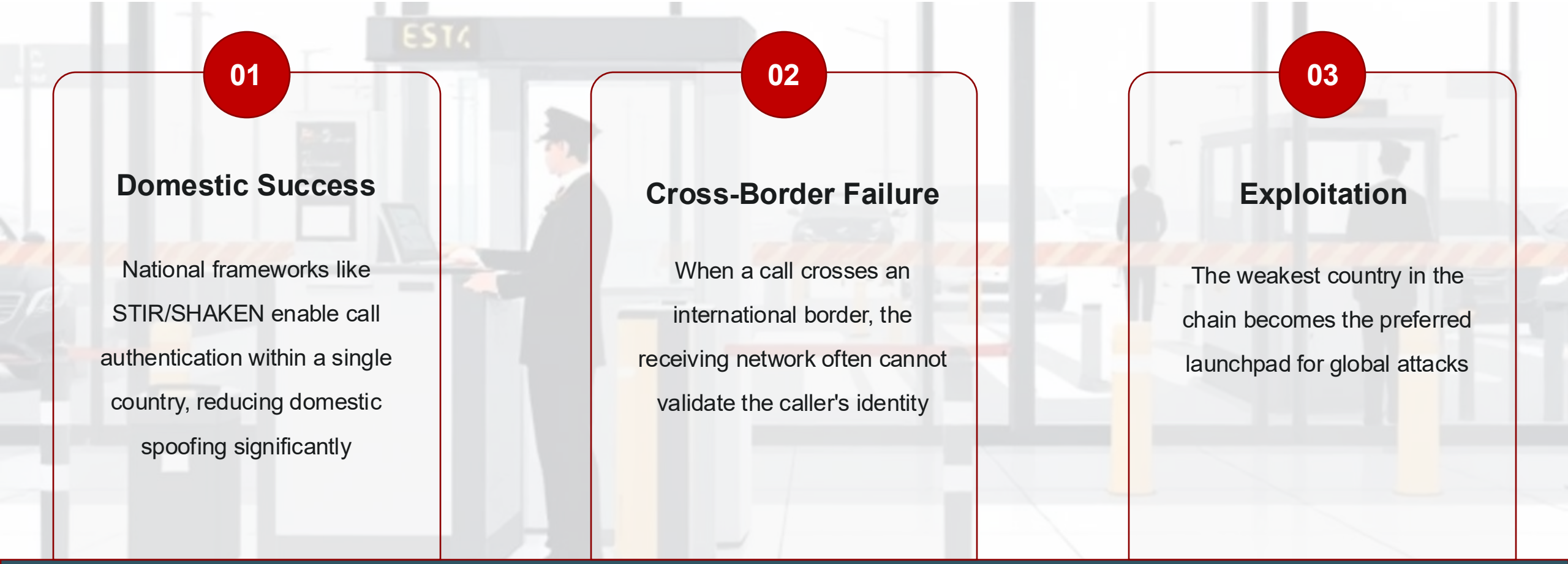
Enterprises can safely communicate with customers without fear of brand impersonation

Regulatory Enforcement

Better traceability and enforcement tools for telecom providers and authorities

Think of it like Know Your Customer (KYC) in the financial sector. A phone number or sender ID should only be trusted if we can validate the identity behind it. Without that verification, criminals can route their attacks through any weak point in the global network

The Border Problem: Where National Solutions Break Down



01

Domestic Success

National frameworks like STIR/SHAKEN enable call authentication within a single country, reducing domestic spoofing significantly

02

Cross-Border Failure

When a call crosses an international border, the receiving network often cannot validate the caller's identity

03

Exploitation

The weakest country in the chain becomes the preferred launchpad for global attacks

Critical gap: Legitimate calls may be blocked while fraudulent calls are accepted. We need secure, consistent authentication handoff across jurisdictions at scale.

Building the Foundation: Identity, KYB, and Interoperability

Authentication systems are only as reliable as the trust infrastructure behind them. That trust begins with rigorous identity verification.

Essential Requirements

Know Your Business (KYB)
processes to vet organizations behind phone numbers, short codes, and sender IDs

Know Your Customer (KYC)
safeguards ensuring individual end users are not anonymous

Auditable registries
for numbers, brands, and messaging assets with full transparency

It is not enough to say a call is "signed." We must also trust the entity behind the signature. When telecom and financial systems adopt aligned identity standards, we create a shared foundation that makes authentication portable and stops fraud before it starts.

The Ecosystem Imperative: Collaboration Across Borders

Standardized KYB

Vetting enterprises through consistent frameworks

International Trust

Creating interoperable systems

Trusted Registries

Maintaining integrity and transparency

Governance Policies

Defining validation and exchange protocols

Warning: If even one link in the chain lacks these protections, it becomes the attacker's entry point. Global security is only as strong as the weakest national framework.

iconectiv's Cross-Border Call Authentication (CBCA) Initiative

1

Verified Caller Identity

Authenticated in the originating country with full KYB validation

2

Portable Credentials

Identity recognized across borders without re-vetting

3

Global Trust Layer

Aligned with national frameworks while enabling international interoperability

Many countries are advancing national programs like verified caller ID and trusted sender registries. CBCA provides the bridge—enabling these systems to recognize and trust each other's authentication credentials seamlessly.

The Path Forward: Making Trust Portable

No Single Entity Can Solve This Alone

We need CSPs, enterprises, regulators, and standards bodies to unite around a minimum set of global authentication standards.

Make Trust Portable

Enable seamless identity handoff across jurisdictions

Make Fraud Unprofitable

Close the gaps that criminals exploit today

Restore Confidence

Rebuild public trust in voice communications

The time to act is now.

Every day we delay, billions more are stolen and thousands more victims lose faith in the phone system. Together, we can restore confidence in every call—no matter where it comes from