Cross Industry Timing in the Fight Against SCAM/SPAM

Tom Cast

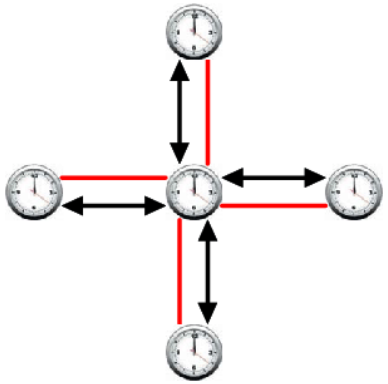
Sr. Director Core Service Engineering

T-Mobile

Why This Matters to This Room

Digital Trust Depends on Synchronized Systems

- Modern telecom operates as a distributed system
- Trust depends on sequencing, validation, and coordination
- Fraud mitigation relies on these principles



The Fraud Landscape Has Changed

Fraud Is Cross-Channel and Cross-Ecosystem

Fraud Campaign Movement

- Campaigns move across channels
- Cross-border and automated
- Fraud operates as a coordinated system

Industry Progress Is Real

Significant Safeguards Are in Place

- STIR/SHAKEN
- SMS firewalls
- Threat intelligence
- Regulatory coordination

Regulation

Authentication

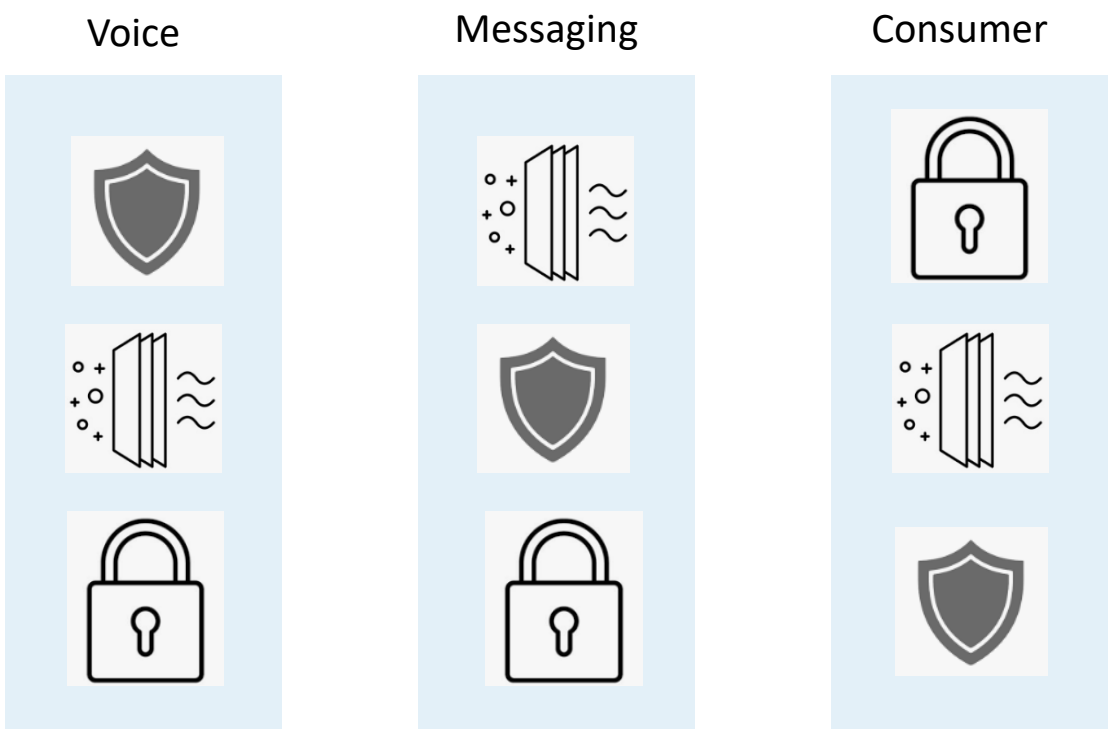
Messaging Protections

Network Controls

We Already Have Controls

The Industry Has Built Stronger Defenses

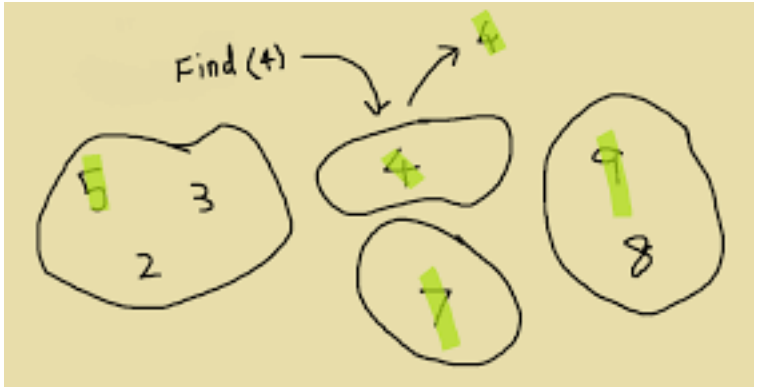
- Voice:
  - CLI protection
  - DNO
  - Firewalls
- Messaging:
  - SMS firewall
  - sender ID
  - URL blocking
- Customer: SIM swap, reporting, APIs
- Controls are extensive — but often domain-specific



The Core Challenge

Fraud Is Synchronized. Defense Is Fragmented.

- Detection happens in one channel
- Delayed action in another
- Intelligence is not shared consistently
- Response timing varies across ecosystems
- Fraud flows to weakest point

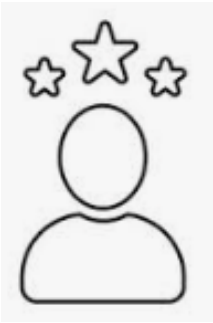


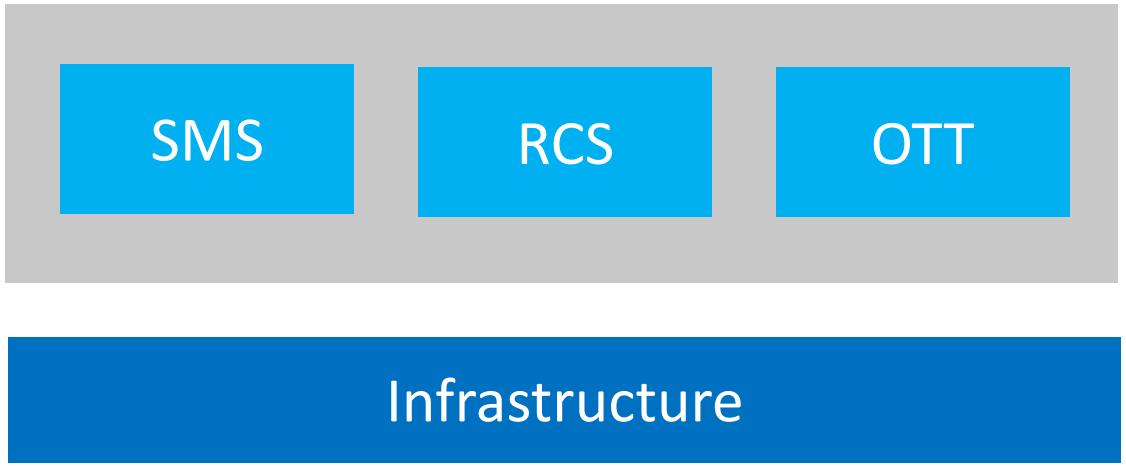
The Messaging Ecosystem Today

One User Experience — Multiple Ecosystems

- Operator Domain → (Voice, SMS)
- Google → RCS
- Apple → iMessage

- Users see one conversation layer
- Fraud sees one attack surface
- Defenses are still segmented





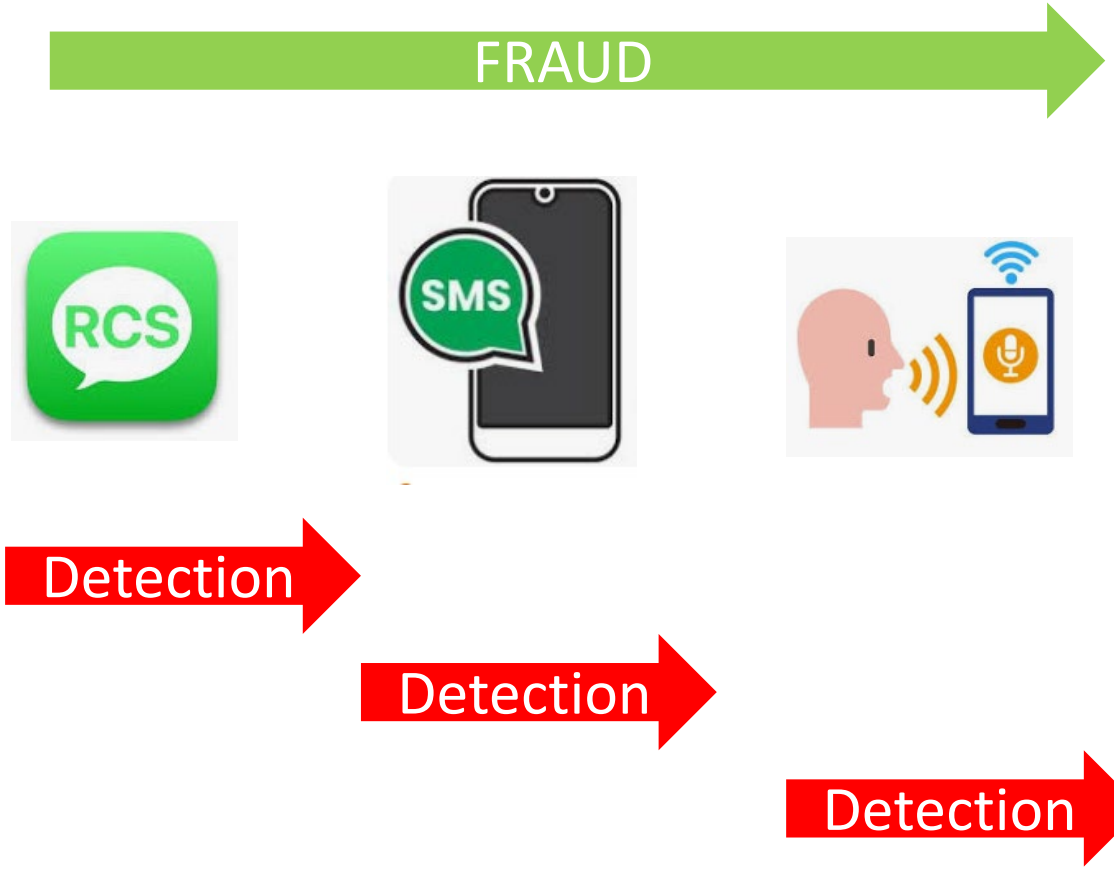
Where Timing Gaps Emerge

Coordination Challenges Create Exploitable Windows

Example flow:

- Fraud detected in RCS
- Actor pivots to SMS
- Then escalates to voice spoofing
- Signal does not propagate fast enough

- Fraud operates in real time — coordination does not



Real Life Example

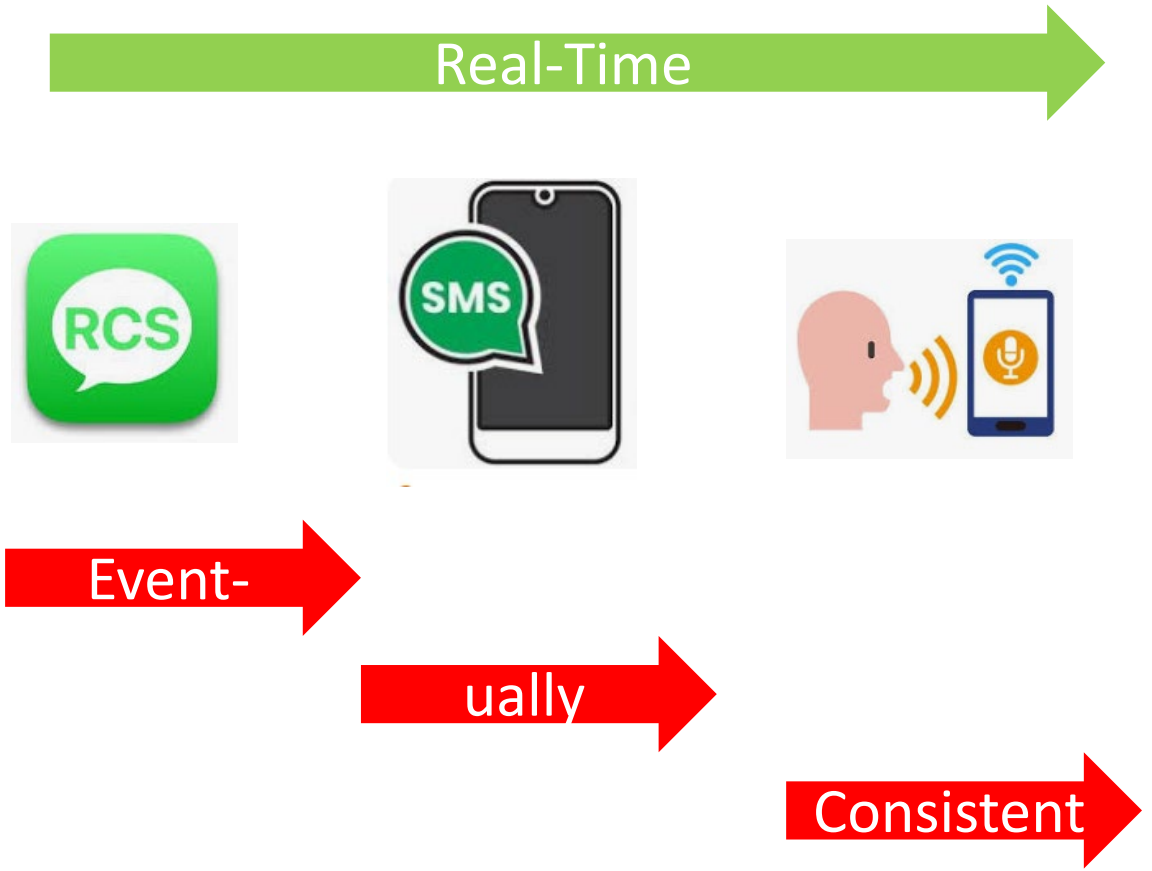
Slow Coordination Challenge

The Synchronization Problem

Eventually Consistent Defense vs Real-Time Adversary

- Signal discovery is delayed
- APIs are not fully interoperable
- Identifications differ across platforms
- Response SLAs are not aligned

Fraud exploits timing gaps between systems



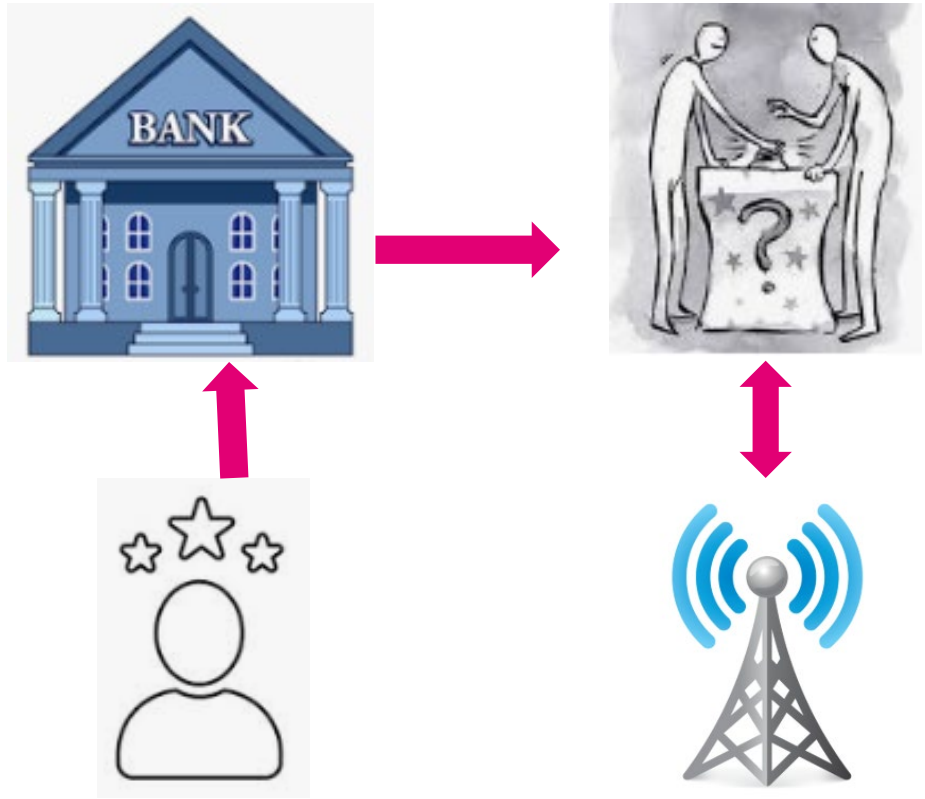
Example: Cross-Industry Coordination

Fraud Signal Integration in Financial Services

Scenario:

- Customer initiates high-value transaction
- Bank queries telecom network
- Detects active suspicious call
- Transaction paused or verified

Cross-industry synchronization improves outcomes

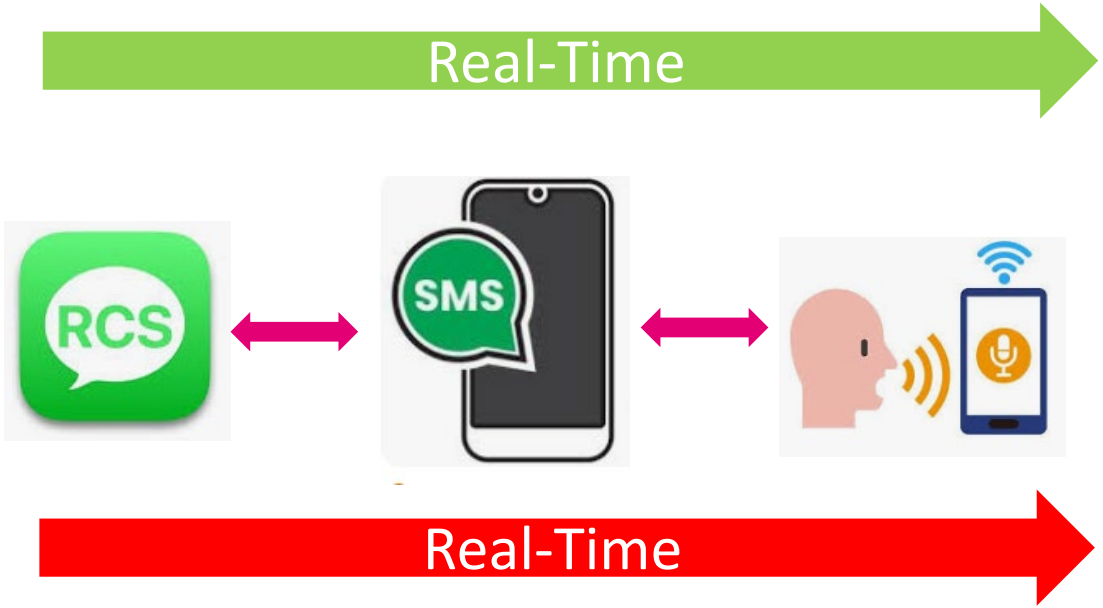


What Synchronized Action Looks Like

From Controls to Coordination

- Shared fraud signal identification
- Faster intelligence exchange
- Cross-platform signal propagation
- Aligned response timing thresholds
- Joint incident review and learning

Coordination is the next maturity step

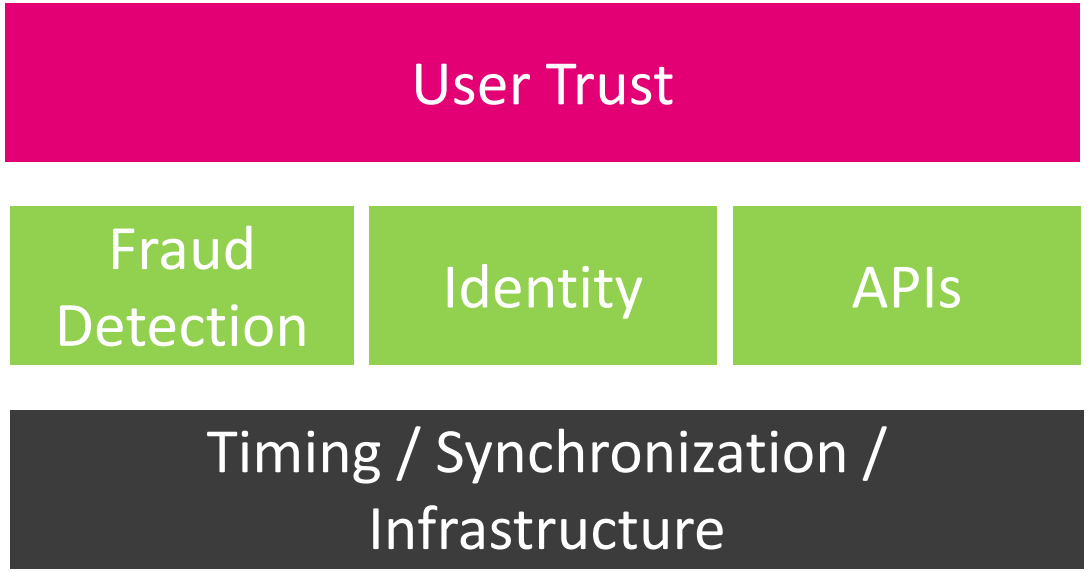


The Role of Infrastructure

Synchronization Underpins Trust

- Event sequencing
- Better timestamp integrity
- Better system consistency
- More reliable signal propagation

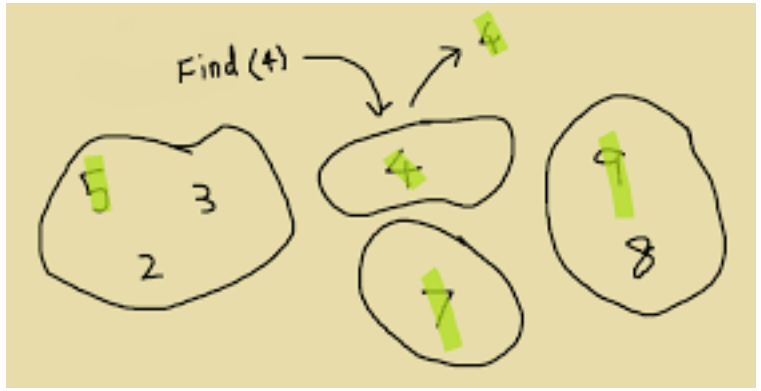
Fraud defense behaves like an eventually consistent system.
Fraud operates in real time.



The Opportunity

Move From Channel Protection to Ecosystem Trust

- Reduce cross-platform blind spots
- Improve speed of response
- Strengthen attribution and accountability
- Build more consistent user trust



Transition

The Risk Ahead

Fraud Velocity Is Increasing

- AI-generated voice and messaging
- Real-time cross-platform campaigns
- Fraud-as-a-service ecosystems
- Increased automation

Coordination must accelerate

In Closing

Fraudsters Are Synchronized Across Platforms
Our Defenses Must Be As Well

Synchronizing infrastructure was the first step.
Synchronizing action is the next.