Firebase PNV | HCLTech

ANTI-FRAUD & NETWORK API MONETIZATION

Two Sides of the Same Coin

How Carrier-Verified Phone Numbers Stop Fraud and Create New Network API Revenue



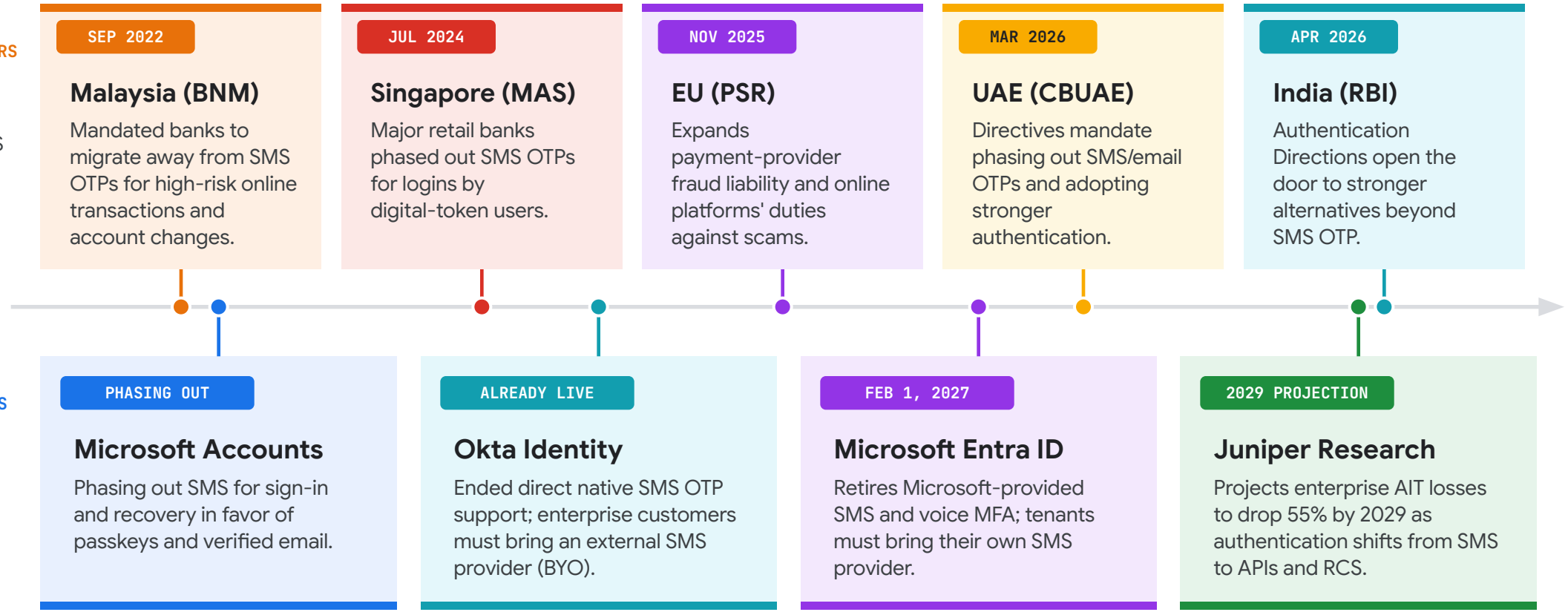
Micah Baker
Sr. Product Manager, Firebase

ONE CAPABILITY • TWO OUTCOMES
Side 01: Anti-Fraud Protection | Side 02: Network API Revenue

01 // THE MARKET SHIFT

Regulators and Identity Platforms Are Phasing Out SMS OTP

Financial regulators and major authentication platforms are actively phasing out SMS codes.



Sources: BNM (2022); MAS/ABS (Jul 2024); EU PSR provisional agreement (Nov 2025); CBUAE Notice 2025/3057; RBI Directions 2025; Juniper Research.

KEY TAKEAWAY: Authentication traffic is leaving SMS OTP regardless. Network APIs let operators capture that demand instead of losing it.

02 // THE FRAUD LANDSCAPE

Phone Fraud Follows the Phone Number Across Every Channel

Four high-cost attack patterns that operator fraud and revenue assurance teams manage every day.

SIM SWAP SURGE

+1,055%

Unauthorised SIM Swaps

- Unauthorised SIM swap cases rose 1,055% YoY in the UK (almost 3,000 cases in 2024, Cifas).
- Fraudsters hijack a subscriber's number to intercept banking and account recovery OTPs.

ACCOUNT TAKEOVER

+76%

Account Takeover

- Account takeover cases rose 76% in 2024; telecoms ATO up 105% (Cifas).
- Compromised phone numbers act as the skeleton key to downstream digital accounts.

SMS PUMPING / AIT

$2.1B

Artificially Inflated Traffic

- Enterprises lost $2.1B to SMS pumping in 2023 (Juniper Research).
- Automated bots trigger millions of paid OTP messages across high-cost and grey routes.

SMISHING SCAMS

$470M

SMS Phishing Losses

- $470M in reported US text-scam losses in 2024—5× the 2020 total (FTC).
- Subscribers are social-engineered into typing or forwarding 6-digit SMS codes.

KEY TAKEAWAY: Global telecom fraud reached $41.8B in 2025 (CFCA)—and the 6-digit SMS code sits at the center of these attacks.

Sources: CFCA Global Fraud Loss Survey (Dec 2025, $41.82B); Cifas Fraudscape 2025 (UK 2024 vs 2023); Juniper Research (AIT 2023); US FTC Consumer Sentinel (2024).

03 // A NEW GENERATION

Firebase PNV: The Third Generation of Phone Verification

Cryptographic carrier verification confirmed with one tap—working over any internet connection.

▲ SECURITY + REACH

Each step eliminates fraud and broadens reach.

GEN 1 // LEGACY MESSAGING

SMS OTP

HOW IT VERIFIES
Sends a human-readable 6-digit code over messaging routes.

CONNECTIVITY
Requires cellular SMS delivery; fails without mobile network coverage.

USER EXPERIENCE
High friction: wait, switch apps, read, and manually type 6 digits.

FRAUD EXPOSURE
Exposed to smishing, AIT bot pumping, SS7 interception & SIM swap.

GEN 2 // PRE-TS.43 NETWORK

Silent Network Auth

HOW IT VERIFIES
Checks active cellular data session via mobile IP redirects.

CONNECTIVITY
Requires active cellular data connectivity.

USER EXPERIENCE
No manual code, but lacks a standardized OS-level consent sheet.

FRAUD EXPOSURE
No SMS code to phish, but limited reach without active cellular data.

GEN 3 // MODERN STANDARD (TS.43)

Firebase PNV

HOW IT VERIFIES
Device SIM proves possession directly to carrier via GSMA TS.43.

CONNECTIVITY
Works on ANY internet connection—Wi-Fi or mobile data.

USER EXPERIENCE
Explicit 1-tap Android consent sheet; verified in ~1–3 seconds.

FRAUD EXPOSURE
Nothing to phish, nothing to pump; billed only on success.

KEY ADVANTAGE · ZERO PHISHING
Wi-Fi + Mobile Reach · ~1–3s Verification

KEY TAKEAWAY: Firebase PNV combines explicit 1-tap user consent with cryptographic SIM proof, and works over both Wi-Fi and mobile data.

04 // NUMBER CONFIDENCE

Not all verified numbers mean the same thing

Only Firebase PNV confirms the number on the device running the app

PASSIVE

SMS OTP

"This user has access to this number."

- The code can be read on any device or forwarded to an attacker
- You can't tell which device or person holds the SIM
- A correct code shows past access, not where the SIM is right now

INDIRECT

Silent network authentication

"A request came over this number's mobile connection."

- Checks the network path, not the device running the app
- A proxy on the victim's phone can relay an attacker's request over that connection
- Requires active cellular data connectivity; otherwise apps fall back to SMS

DIRECT

Firebase PNV

"This is the phone number on the device running the app right now."

- The operator confirms the number for the SIM in this device
- The result returns to the app on that device after one consent tap
- Your app receives a signed, verifiable result

KEY TAKEAWAY: Firebase PNV ties the verified number to the device your app is running on.

05 // THE WEAK LINK

Why SMS OTP Is the Weak Link in Digital Identity

A human-readable code sent over messaging can be pumped, intercepted, redirected, or phished.



App requests a code

ATTACK 1 · PUMPING

Bots pump paid SMS

Bots hit public sign-up and login forms to trigger paid OTP traffic. The enterprise pays for every fake message.

Code crosses networks

ATTACK 2 · TRANSIT

Codes read in transit

Plaintext 6-digit codes hop across SS7, aggregators and grey routes, where they can be intercepted or delayed.

Code lands on a SIM

ATTACK 3 · SIM SWAP

SIM swap steals the code

A fraudster social-engineers a SIM swap or number port-out, so the code arrives on the attacker's device.

User types the code

ATTACK 4 · PHISHING

Phishing captures it

Because the code is human-readable, fake sites and callers trick subscribers into typing it for them in real time.

WHO PAYS THE PRICE

SUBSCRIBERS

Hijacked accounts, lost time

Stolen bank, social and shopping accounts, plus the wait, app switch and 6-digit typing.

ENTERPRISES

Fraud bills and lost sign-ups

Unpredictable AIT bills from bot pumping, and real users drop off when codes arrive late.

OPERATORS

A2P SMS trust erodes

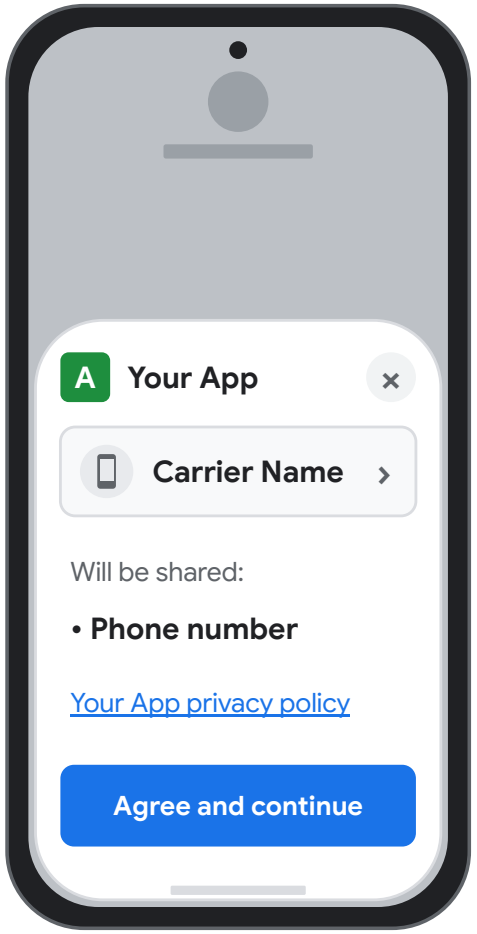
Enterprises cap SMS spend or move to app-based options; smishing erodes network trust.

KEY TAKEAWAY: SMS was built for person-to-person messaging, not identity, and fraudsters exploit every step of the code's journey.

06 // HOW IT WORKS

Verified by the Carrier, Confirmed with One Tap

A verified phone number returned to the app in ~1–3 seconds—with the operator as the root of trust.



1 **Eligibility Check** — FIREBASE SDK
Firebase SDK checks on-device that the SIM and operator network are supported; if not, the app falls back seamlessly.

2 **One-Tap Consent** — ANDROID OS
Android presents a system consent sheet with the app's verified brand; the user taps "Agree and continue" once.

3 **SIM Authentication** — MOBILE OPERATOR
The SIM authenticates with the operator entitlement server over any internet connection to confirm active possession.

4 **Signed Token** — GOOGLE BACKEND
Google returns a cryptographically signed JWT containing the verified MSISDN to the enterprise backend in ~1–3s.

THREE PILLARS OF TRUST · ROLES & VALUE EXCHANGE

OPERATOR ROLE
Authoritative Root of Trust
Verifies SIM possession at its network endpoint and earns revenue on every successful verification.

FIREBASE PNV ROLE
Global Scale & Abuse Layer
Provides SDK, Android consent UX, brand vetting, billing, and anti-abuse protection.

ENTERPRISE APP ROLE
Integrate Once, Reach Globally
Integrates once; newly launched operator networks start working automatically.

KEY TAKEAWAY: The mobile operator stays the authoritative root of trust, while Firebase brings global developer demand.

07 // FRAUD IMPACT

How Carrier Verification Closes the Gaps Fraudsters Exploit

What changes across each major fraud pattern when the 6-digit SMS code is removed.

Smishing & OTP Phishing	SMS OTP: Users tricked into typing or forwarding 6-digit codes. **With Firebase PNV:** No shareable code exists—SIM possession is verified cryptographically on-device.	ELIMINATED
SMS Pumping (AIT)	SMS OTP: Bots trigger millions of paid SMS messages to high-cost ranges. **With Firebase PNV:** No SMS is sent; requires an on-device SIM tap, and businesses pay only on success.	ELIMINATED
Transit Interception (SS7 / Grey Routes)	SMS OTP: Plaintext codes exposed across signalling and aggregator hops. **With Firebase PNV:** End-to-end encrypted proof between the device SIM and home operator; signed JWT to app.	CLOSED
SIM Swap & Account Takeover	SMS OTP: Swapped SIM silently receives recovery codes on attacker's phone. **With Firebase PNV:** Proves live SIM possession now—and pairs with operator SIM Swap API signals for high-risk flows.	STRONGER TOGETHER

KEY TAKEAWAY: Carrier verification removes the code that phishers and pumpers target—and sets the foundation for SIM Swap risk signals.

08 // LIVE DEMO

Live Demo: Carrier-Verified Sign-Up on Pixel 9a

Side-by-side comparison using a live Google Pixel 9a provisioned with multiple carrier eSIMs.

TIME AXIS →

LEGACY FLOW
SMS OTP
6 steps

- 1 · ENTRY — **Select Country** & type phone number
- 2 · A2P — **Trigger A2P** App sends paid SMS
- 3 · SMS TRANSIT DELAY — **Wait for Delivery** Aggregator routing and network hops
- 4 · SWITCH — **Switch Apps** Open app to read code
- 5 · MEMO — **Memorize** Remember 6 digits
- 6 · VERIFY — **Type Digits** Enter code in form
- × OUTCOME — **Slow Result** High drop-off · Phishable

FIREBASE PNV
Pixel 9a
1 tap · ~1–3 s

Tap | Agree | SIM ✓ | Verified ✓ (~1–3 s)

REST OF THE FLOW ELIMINATED · ZERO SMS SENT

1 · Tap 'Verify' — In-app button
2 · Tap 'Agree' — Android OS consent
3 · SIM Verified Over Wi-Fi — Authenticates with SIM

WHAT TO WATCH FOR IN THE LIVE DEMO

SEAMLESS USER EXPERIENCE

Zero Typing & Zero App Switches

Users never leave the sign-up flow to open Messages, memorize a 6-digit code, or type numbers manually. One tap on the Android consent sheet completes verification.

ANY INTERNET CONNECTION

Works Over Venue Wi-Fi

Carrier verification runs over any internet connection, including the venue Wi-Fi, with no cellular data required.

SIM-BASED SECURITY

No SMS Sent, Nothing to Phish

The Pixel 9a's operator eSIM authenticates directly with the home operator. There is no SMS to intercept, pump or phish.

KEY TAKEAWAY: Watch the live Pixel 9a demo: verification completes in ~1–3 seconds over Wi-Fi with zero SMS messages sent.

Proven at Scale and Live Across 12 Countries Today

Production benchmarks from Google 1P and customer A/B testing—plus every live carrier network today.

GOOGLE 1P BENCHMARK



Verification Success
trending to 98% over 3 months

Google first-party deployments run at ~95–98% global verification success, with no international SMS routing failures.

CUSTOMER A/B TEST VS. SMS

Higher End-to-End Conversion

With a pre-consent explainer screen, user click-through rate matched SMS OTP while verification success was significantly higher on Firebase PNV.

`Click-through rate: matched (1.0x)`

Firebase PNV · significantly higher verification

SMS OTP · baseline

EUROPE · 9 COUNTRIES

Developers integrate once; every newly launched network activates automatically.

Germany
Deutsche Telekom, Vodafone, Telefónica O2, MagentaMobil, Congstar / Fraenk, EDEKA smart, Penny Mobil, Kaufland mobil, NORMA connect

United Kingdom
Vodafone

France
Orange

Spain
Telefónica, MasOrange

Netherlands
VodafoneZiggo

Finland
DNA

Ireland
Vodafone

Greece
Vodafone

Romania
Vodafone

ASIA-PACIFIC · 3 COUNTRIES

Indonesia
Telkomsel

Malaysia
CelcomDigi, U Mobile, Tune Talk

Pakistan
PTML (Telenor)

KEY TAKEAWAY: "...helping developers innovate faster and accelerating Network API adoption across Europe." — Johanna Wood, Vodafone

Sources: Firebase Phone Number Verification Supported Carriers documentation & Firebase Blog, 28 Sep 2026 (Johanna Wood, Director of Network APIs, Vodafone).

ROPE: the Regional Onboarding Policy Engine

Part of Firebase PNV, it decides which developers can verify numbers in each region and checks every request

R Regional

WHERE

Each region has its own policy, so numbers follow rules written for their region.

O Onboarding

WHEN

Developers are vetted in the Firebase console before their first number verification.

P Policy

WHAT

It sets what developers must prove, such as the TMF931 fields and a business identity match.

E Engine

HOW

Software applies the rules automatically, at onboarding and on every verification request.

WHO RUNS IT

Firebase runs ROPE as part of Firebase PNV, on every project that verifies numbers, in every region.

One policy, applied consistently to every developer on every request.

ROPE turns each region's policy into automatic checks

The Regional Onboarding Policy Engine applies each region's policy to every Firebase project

01

Set regional policy

The TMF931 fields, business verification and sanctions rules form a region's policy.

ONE POLICY PER REGION

02

Collect evidence

At onboarding, ROPE fills answers from Google and trusted business records, and checks what the developer declares.

AT ONBOARDING

03

Enforce every request

Before a number is returned, ROPE confirms the project is approved for that region.

EVERY REQUEST

04

Monitor and suspend

A sanctions update or a failed re-check can suspend access and notifies the owners.

ONGOING

PRE-FILTERED

Developers only see the paths they qualify for, so nobody wastes a verification attempt.

The rules run before the first verification and on every request after it.

Approval is the start, not the end

ROPE keeps checking every project for as long as it verifies numbers



EVERY REQUEST

Checked each time

Each verification confirms the app's signing identity, verified brand and regional approval before a number is returned.



EVERY CHANGE

Re-checked on change

Sanctions updates and changes to a developer's business records trigger a fresh check automatically.



ON A SCHEDULE

Re-confirmed

Developers periodically re-confirm contacts, data location and purpose.



IF A CHECK FAILS

Suspension

A failed check can suspend the developer's access and notifies the project owners.

What ROPE re-checks

- **Business records from trusted registries**
- **Sanctions lists as they update**
- **App signing identity on every request**

A form is a snapshot; ROPE keeps checking for as long as the app verifies numbers.

ROPE opens three new go-to-market opportunities

Because ROPE vets every developer, operators can monetize anti-fraud in three new ways

1



Domestic and international rates

Separate rates for domestic and international businesses.

ROPE CHECKS

Where the parent company is based

2



MAU security checks

One paid PNV a month unlocks silent security checks, billed per active number.

ROPE CHECKS

Each developer's verification level

3



Third-party platforms

Security platforms and cloud providers offer Firebase PNV to their developers through one agreement.

ROPE CHECKS

Every platform developer

Knowing every developer is what makes each opportunity safe for your network.

Today, Only International Apps Get the Easy Path

Where Firebase PNV serves only international apps, domestic apps integrate with each operator separately

INTERNATIONAL APPS · TODAY

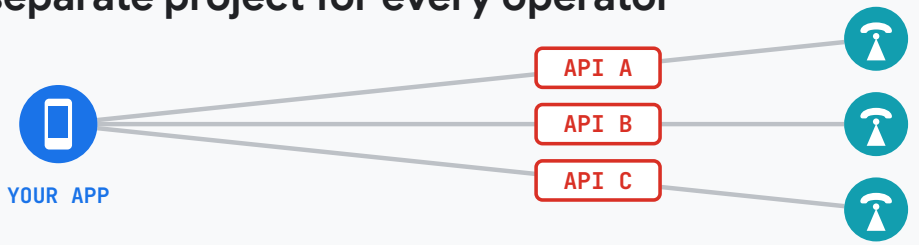
One integration reaches every operator



- **One SDK**
  The Firebase PNV SDK works the same on every network.
- **Centralized billing**
  One bill from Google, whatever the network.
- **Centralized support**
  One place to get help.

DOMESTIC APPS · TODAY

A separate project for every operator



- **Different APIs**
  Each operator's API may work differently.
- **Separate contracts and bills**
  A commercial agreement and invoice per operator.
- **Separate support**
  A different contact for every network.

THE GOAL

Serve domestic apps through Firebase PNV too, so every developer can adopt the same security improvements.

KEY TAKEAWAY: Bringing domestic apps onto Firebase PNV gives every developer the same easy path to stronger security.

ROPE knows where each business's parent company is based

The global parent comes from a trusted business record, so rates can differ for domestic and international businesses

A business onboards

ROPE checks the global parent

From the business record

RATES CAN FOLLOW THE PARENT COMPANY

Parent based in the operator's country

DOMESTIC RATE

Parent based in another country

INTERNATIONAL RATE

HOW ROPE CLASSIFIES

Subsidiaries are linked

A local branch of a foreign company is linked to its global parent.

One source of truth

The parent company comes from the same business record ROPE matches.

Applied on every request

ROPE applies each developer's classification whenever a number is verified.

Knowing every parent company makes separate domestic and international rates possible.

16 // NEW MAU MODEL

One Paid PNV a Month Unlocks Ongoing Security Checks

A new monthly active user (MAU) model turns anti-fraud checks into recurring operator revenue.

1

STEP 1 · PAID PNV

One verification per month

A transactional PNV verifies the number, and the user agrees to fraud monitoring. One PNV a month activates MAU for that app and number.

2

STEP 2 · MAU CHECKS

Silent security checks all month

With no user prompt, the app checks the number at sign-in, recovery and checkout, within usage limits. Each journey calls only the network APIs it needs, e.g. SIM swap or number recycling.

3

STEP 3 · MONTHLY RESET

Renews every calendar month

MAU resets each month. A fresh PNV and consent re-activate it, so every active number earns again.

HOW OPERATORS EARN

PNV revenue

Every transactional PNV is paid, as today.

MAU revenue, on top

A monthly charge per app per active number. Firebase provides MAU identifiers and numbers for reconciliation.

KEY TAKEAWAY: Anti-fraud becomes recurring revenue: one paid PNV a month opens MAU security checks, billed on top.

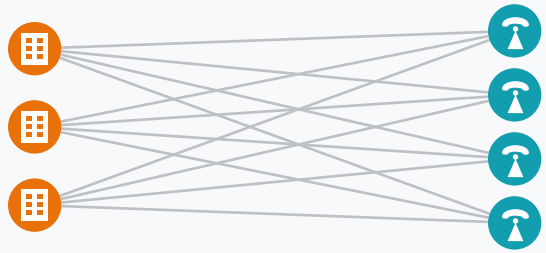
Platforms reach every operator through Firebase PNV

A go-to-market goal: security platforms and cloud providers offer Firebase PNV to their developers

WHY PLATFORMS WANT THIS

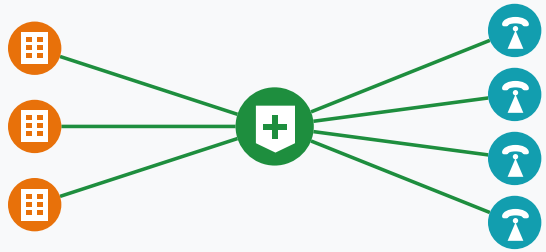
One agreement, not dozens

WITHOUT FIREBASE PNV



Each platform contracts with every operator.

WITH FIREBASE PNV



One agreement reaches every operator.

HOW IT FLOWS DOWN

Your network → **Firebase PNV** (ROPE) → **Platform** (e.g. security platforms, cloud providers) → **Platform's developers**

SAME VETTING

Every platform developer passes ROPE

Firebase runs every ROPE check on every developer, including platforms.

SAME TERMS

Service terms flow down

The Firebase PNV service terms apply to every platform developer.

SAME LIMITS

Limits follow verification level

Platform developers get the same usage limits as direct developers.

Platforms reach every operator through one agreement, and every developer still passes ROPE.

Anti-Fraud and Monetization: One Capability, Two Wins

The same carrier verification that protects subscribers from fraud also creates new Network API revenue.

SIDE 01 // ANTI-FRAUD

Protect Subscribers & Trust

Value for Fraud Management Leaders

• Stops OTP Phishing & Smishing: Removes the shareable 6-digit code that social engineers target.

• Eliminates SMS Pumping (AIT): No SMS is sent; bots cannot trigger unverified traffic charges.

• Reduces Account Takeover Harm: Cryptographic SIM proof pairs with SIM Swap detection.

• Regulatory Alignment: Supports central bank and EU PSR anti-fraud goals.



SHARED FOUNDATION

Carrier-verified phone number + network fraud signals exposed once via Firebase PNV.

SIDE 02 // NETWORK API REVENUE

Monetize Every Verification

Value for Revenue & Commercial Leaders

• Per-Verification API Revenue: Earn high-margin revenue for every successful verification.

• Turnkey Global Demand: Reach Firebase's global app developer ecosystem with zero sales buildout.

• Capture Post-OTP Migration: Retain authentication value as platforms phase out SMS OTP.

• Expand Lifecycle APIs: Upsell SIM Swap, Number Recycling, and KYC signals.

KEY TAKEAWAY: Fraud prevention and Network API monetization are not competing priorities—they are two sides of the same coin.

Four Moves for Fraud and Revenue Leaders

Practical actions to stop phone-number fraud and unlock Network API revenue.

01

MOVE 01 // VISIBILITY

Separate OTP from Total A2P SMS

WHAT TO DO

- Many operators do not currently split out authentication OTP volume from overall A2P messaging.
- Baseline your OTP traffic and AIT pumping exposure before regulatory and platform shifts accelerate.

OUTCOME

✓ Baseline Revenue at Risk

02

MOVE 02 // ALIGNMENT

Bridge Fraud & Network API Teams

WHAT TO DO

- Connect Fraud Management / Revenue Assurance directly with your Network API commercialization team.
- Treat carrier number verification as both a subscriber protection control and a revenue product.

OUTCOME

✓ Shared Identity KPI

03

MOVE 03 // COMMERCIALIZATION

Connect to Firebase PNV Demand

WHAT TO DO

- Partner with Firebase PNV to tap into immediate demand from global apps and enterprises.
- Leverage existing network entitlement capabilities rather than building custom developer channels.

OUTCOME

✓ Per-Verification Revenue

04

MOVE 04 // EXPANSION

Layer High-Value Fraud Signals

WHAT TO DO

- Build on Phone Number Verification by exposing SIM Swap and Number Recycling signals.
- Protect high-risk banking logins, account recovery, and payment transactions.

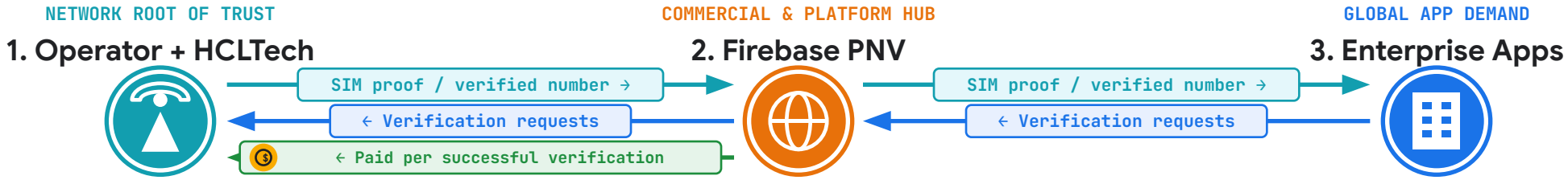
OUTCOME

✓ Full Lifecycle Value

KEY TAKEAWAY: Protect your subscribers from fraud and grow Network API revenue, with the same investment.

How Operators Participate: Operator × HCLTech × Firebase

Combining operator network trust and fraud assurance with Firebase's global developer channel.



- **Fraud & revenue intelligence**
  Monitor fraud patterns, size AIT exposure, and assure the new API revenue stream.
- **Network enablement**
  Expose phone number verification from the operator's entitlement server when ready.

- **Commercial partnership**
  Direct agreement paying the operator for every successful verification.
- **Turnkey platform**
  Developer onboarding, brand vetting, Android consent UX, billing and abuse defense.

- **Single SDK integration**
  Banks, fintechs, commerce, and social apps integrate once with Firebase.
- **Automatic activation**
  Every newly launched operator network begins serving traffic automatically.

OPERATOR ONBOARDING TRACK // 4 STEPS TO LIVE REVENUE

01 · AUDIT
Size OTP & AIT Exposure
Separate auth SMS from total A2P volume to quantify fraud risk.

02 · PARTNER
Align Commercial Terms
Establish commercial terms with Google to monetize API calls.

03 · CONNECT
Enable & Certify TS.43
Expose verification endpoint with Google.

04 · MONETIZE
Go Live Automatically
Firebase apps verify subscribers and generate new API revenue.

KEY TAKEAWAY: Operators don't need to build a developer salesforce. HCLTech helps assure the network while Firebase brings global app demand.

OPEN DISCUSSION & Q&A // HCLTECH REVENUE INTELLIGENCE USER FORUM

Thank You & Discussion

Stopping Phone Fraud and Growing Network API Revenue Together

DISCUSSION QUESTIONS FOR THE ROOM

- Visibility: Do your teams have a clear split between SMS OTP volume and total A2P messaging today?
- Regulation: How are banking and telecom regulators in your markets approaching SMS OTP fraud?
- Alignment: How closely connected are your Fraud Management and Network API monetization teams?



Micah Baker • Sr. Product Manager, Firebase
Documentation & Live Networks:
firebase.google.com/docs/phone-number-verification
HCLTech Revenue Intelligence & Telecom Presales Team

APPENDIX A1 // CONSENT UX & CONVERSION

Why a Pre-Consent Explainer Screen Drives Conversion

Customer A/B testing shows setting context before the OS prompt matches SMS CTR and lifts completion.

EARLY ADOPTER LEARNING

Unannounced Prompts Drop Off

Parallels to early Passkey rollouts

• Early adopters report user drop-off when an unfamiliar OS consent screen appears without context.

• We observed the exact same pattern during the initial rollout of Passkeys.

• Users hesitate when a system sheet asks to share identity data unexpectedly.

PRODUCTION A/B TEST

Head-to-Head vs. SMS OTP

Controlled customer experiment

• A Firebase PNV customer ran a production A/B test comparing SMS OTP against Firebase PNV.

• Click-Through Rate (CTR): Identical across both the SMS group and the Firebase PNV group.

• Verification Success Rate: Significantly higher on Firebase PNV once users consented.

BEST-PRACTICE UX PATTERN

Pre-Consent Explainer

Prepare the user before the OS sheet

• Place a lightweight explainer screen immediately ahead of the Android consent prompt.

• Sets clear expectation: "Verify your number in one tap with your mobile carrier—no SMS code required."

• Turns an unfamiliar prompt into a high-conversion 1-tap confirmation.

KEY TAKEAWAY: Adding a pre-consent explainer screen matches SMS OTP click-through while delivering far higher verification success.

APPENDIX A2 // DEVELOPER ADOPTION TIMELINES

Real-World Developer Timelines to Adopt Verification

Three empirical engineering scenarios observed across apps integrating carrier phone verification.

SCENARIO 1 // ~1 MONTH DEV TIME

Add Phone Numbers to Existing User Accounts

Lowest-friction entry point: step-up verification, account recovery, or binding a verified phone number to an existing logged-in account. Requires minimal changes to core auth state and ships in ~1 month.

SCENARIO 2 // ~3 MONTHS DEV TIME

Add Firebase PNV to All New User Sign-Up & Sign-In Flows

Full integration across primary onboarding and login flows on an existing app—including pre-consent explainer screens, SMS fallback orchestration, and phased A/B rollout across live carrier markets (~3 months).

SCENARIO 3 // ~6 MONTHS DEV TIME

Convert Centralized Email/Password Auth to Phone-First

Architectural transformation: converting a centralized authentication backend that previously required email/password to only require a phone number, plus updating client apps for phone sign-up (~6 months).

KEY TAKEAWAY: Apps often start with 1-month step-up flows and expand to full sign-up/sign-in over 3–6 months—compounding operator API volume.

APPENDIX A3 // EXPANDING NETWORK FRAUD SIGNALS

Expanding Both Sides of the Coin with Fraud Signals

Pairing number verification with operator risk signals protects the full subscriber lifecycle.

SIGNAL 01 // ACCOUNT TAKEOVER

SIM Swap Recency

Detect recent SIM changes

• Fraud Target: Attackers perform an unauthorised SIM swap to hijack bank logins and password resets.

• Operator Signal: Indicates whether the SIM card bound to this number changed recently.

• Revenue Opportunity: Called on high-risk logins, wire transfers, and credential recovery.

SIGNAL 02 // ACCOUNT HYGIENE

Number Recycling

Verify subscriber continuity

• Fraud Target: Reassigned phone numbers inherit the previous owner's linked accounts and alerts.

• Operator Signal: Indicates whether the number was reassigned after the account was registered.

• Revenue Opportunity: Recurring enterprise checks on dormant accounts and high-value updates.

SIGNAL 03 // ONBOARDING TRUST

Device Swap & KYC Match

Hardware & identity assurance

• Fraud Target: Synthetic identity fraud and stolen credentials during regulated onboarding.

• Operator Signal: Correlates live SIM possession with device continuity or verified operator KYC data.

• Revenue Opportunity: High-margin API calls for banking, fintech, and marketplace onboarding.

KEY TAKEAWAY: Phone Number Verification establishes the commercial channel; SIM Swap and Number Recycling signals monetize the ongoing lifecycle.