Unscammed: Fraud Prevention Network APIs Statement of Requirements

Published: 30 Jun 2026

1. Executive Summary

Scams and authorised push payment (APP) fraud continue to erode trust in digital commerce, banking, and communications. Unscammed is building consumer and enterprise-facing capabilities that help users identify, report, and recover from scams — including automated reporting flows to UK reporting destinations (e.g., Report Fraud / police reporting), bank follow-ups, and preventative tooling including a voice AI companion and scam awareness training.

To move the industry from reactive response to proactive protection, Unscammed seeks operator-verified, real-time network, fraud prevention API signals aligned with the GSMA Open Gateway initiative and CAMARA API standardisation programme. These signals — covering SIM swap events, call forwarding anomalies, number recycling, device changes, and geographic risk — will power a continuously updated scam intelligence engine that is shared in real time with partner banks, fintechs, consumer protection bodies, and law enforcement agencies.

This Statement of Requirements sets out the specific network APIs Unscammed is requesting, the detailed use cases they address, our target markets and deployment timelines, and our commitments on data governance and compliance.

2. About Unscammed

Unscammed - is a fraud-intelligence platform dedicated to detecting, documenting, and disrupting - mobile phone-based scams that target consumers in the United States, Canada, United Kingdom, Australia, South Africa, and India. The platform operates a public reporting channel through which victims and potential victims submit scam phone numbers, messages, and incident details in real time.

Unscammed aggregates these crowd-sourced reports with automated enrichment signals to build a continuously updated threat intelligence database of known and suspected scam numbers. This intelligence is made available to partner organisations — banks, payment service providers, telecommunications providers, consumer protection agencies, and law enforcement bodies — to enable proactive blocking, victim warning, and evidence-based law enforcement referrals.

Unscammed's services support three principal partner segments:

- Banks, PSPs, and fintechs: handling payment authorisation decisions and APP fraud interception, where real-time number risk signals can prevent a fraudulent transfer before it completes.
- Marketplaces and digital platforms: exposed to account takeover, synthetic identity fraud, and social engineering attacks that begin with a phone number.
- Communications and identity workflows: where SIM swap abuse, number recycling risk, and device-account binding checks are required to secure authentication flows.

---

3. Market Gap & Industry Challenges

The "trust gap" in digital transactions

Scammers exploit fragmented identity signals across mobile devices, channels, and institutions. Enterprises currently rely on device fingerprinting, behavioural analytics, and user-reported inputs — useful signals, but not authoritative. Mobile network operators uniquely hold network-level facts (SIM events, call routing state, device changes, geographic position) that can decisively strengthen fraud decisions when exposed safely via standardised Open Gateway network APIs.

Fragmentation and integration cost

Without standardisation, each operator exposes different interfaces, data structures, and policies — increasing cost and dramatically slowing adoption. The GSMA Open Gateway initiative addresses this fragmentation by a common global framework of network APIs based on standardisation and specification by CAMARA with a simplified, consistent integration model. Unscammed is committed to building on this standardised framework rather than bespoke bilateral integrations.

Reporting and recovery are still too complex for victims

Unscammed's consumer-facing offering focuses heavily on simplifying reporting and recovery — an indicator of the real-world friction victims currently face. Earlier prevention, enabled by authoritative network signals, is the only scalable path to reducing the volume of consumers who need to use recovery services in the first place. Network API access is therefore not only an operational requirement for Unscammed but a foundational enabler of the consumer protection mission.

---

4. Outcomes Sought with Network APIs

Through access to the Network APIs described in this document, Unscammed seeks to achieve the following outcomes:

- Reduce scam success rates and fraud losses by enabling real-time risk decisions at key moments: payment authorisation, account onboarding, account recovery, and high-risk communications.
- Improve accuracy and reduce false positives in Unscammed's threat database through authoritative number recycling, number verification, and subscription status signals that prevent innocent subscribers from being mislabelled.
- Produce evidential-quality intelligence packages combining network-level signals (SIM swap timestamps, call forwarding state, roaming country, device information) with consumer report data for law enforcement referral packages that meet evidentiary standards.

- Enable proactive victim protection by subscribing to real-time SIM swap and call forwarding events on monitored numbers, allowing Unscammed and its partners to alert at-risk individuals before harm occurs rather than after.
- Scale internationally by building on GSMA Open Gateway's global API framework and on specification and standardisation of CAMARA, enabling Unscammed - to deploy consistently across United States, Canada, United Kingdom, Australia-, South African and India., And eventually expanding in more countries with operator networks without bespoke per-operator integrations.

5. Network API Requirements

5(a). Requirement from Mobile Operators:

Unscammed calls on mobile network operators in its target markets (see section 6) to expose - the following network APIs aligned with fraud prevention - that can be consumed consistently across networks and countries. The table below sets out each requested API name, its CAMARA identifier, assigned priority, and the specific use case it addresses.

API Name	CAMARA ID	Priority	Unscammed Use Case
SIM Swap	sim-swap	Essential	Query whether a reported number had its SIM swapped in the preceding 24–72 hours — a core indicator of number hijacking and account takeover.
SIM Swap Subscriptions	sim-swap-subscriptions	Essential	Subscribe to real-time SIM swap events so the platform can instantly flag a monitored number at the moment its SIM is changed, enabling proactive partner alerts.
Number Verification V2	number-verification	Essential	Confirm a reported number is genuine and active, preventing fabricated or spoofed numbers from polluting Unscammed's threat intelligence database.
Call Forwarding Signal	call-forwarding-signal	Essential	Detect unconditional call forwarding on reported numbers — technique fraudsters use to intercept victim communications and relay calls through their networks.
Scam Signal (GSMA)	scam-signal	Essential	Ingest operator-certified network-level fraud risk scores to provide an independent corroboration layer alongside Unscammed's crowd-sourced report signals.
Number Recycling	number-recycling	High	Determine if a flagged number changed ownership since the incident date, preventing mislabelling of innocent subscribers who inherited a scammer's number.
Device Swap	device-swap	High	Detect when the physical device linked to a reported number has been swapped — complementing SIM

API Name	CAMARA ID	Priority	Unscammed Use Case
			swap signals with device-level change detection for account takeover analysis.
Device Roaming Status	device-roaming-status	High	Surface geographic anomalies: scammers posing as domestic callers but operating offshore generate high-value discrepancy signals when cross-referenced with claimed identity.
Subscription Status	subscription-status	High	Check whether voice/SMS services are active, suspended, or terminated — contextualising reports and identifying characteristic burner/prepaid account patterns.
Location Verification	location-verification	Medium	Verify that a device is (or is not) in a claimed location, providing cross-check capability for scam calls where origin is claimed to be a specific country or institution.
Location Retrieval	location-retrieval	Medium	Retrieve a device's approximate location for high-confidence scam network attribution, used in conjunction with evidence packages for law enforcement referrals.
Device Identifier	device-identifier	Medium	Link multiple scam reports to a single physical device (via IMEI) across SIM swaps, revealing fleet-level scam operation structure across Unscammed's global report database.

ℹ Priority definitions: Essential = required for Unscammed's core scam-detection engine at launch; High = required for full platform capability within 6 months of launch; Medium = planned for subsequent platform phases and international expansion.

5(b). Requirements from CAMARA - proposed new APIs related to fraud prevention:

Unscammed calls on CAMARA to support the development for following new APIs:

1. Device Authenticity API: Add and support for the existing (and stalled) Device Authenticity API. Device Swap / Device Identifier do not signal if a given device associated with the provided device identifier is subject to any restrictions or risk flags.

2. Call Activity Signal API: Proposal for CAMARA to provide privacy safe Call Metadata / Call Event API - such as whether a call occurred, its timing, duration, direction, or abnormal patterns—without exposing call content or recordings. This would give Unscammed and its partners a new signal to detect suspicious call behaviour, validate scam reports, and identify coordinated fraud activity while remaining compliant with privacy and data protection requirements.

3. Shared Fraud Intelligence API: Proposal to drive the development of a new CAMARA API that would allow trusted third parties, such as Unscammed, to contribute fraud intelligence from their own databases into a standardised framework. This would enable controlled data sharing beyond operator-owned data and support broader industry collaboration on how non-MNO fraud intelligence can be exchanged securely, responsibly, and at scale. Initially, the API could support the sharing of fraudulent mobile numbers, with scope to expand over time to other indicators such as email addresses, mule account numbers, fraudulent links, and websites. Such a framework would help ensure that once a fraud indicator has been identified, which can be used to prevent further harm in future cases. Currently, no standardised cross-border API exists for sharing this type of fraudulent data.

6. Target Countries & Deployment Phases

As mentioned above in section 5(a) with priority as “essential”, Unscammed would like to start working in the following phases with the following priority markets -

Phase 1 — Priority Markets:0–6 months within the current year 2026

Unscammed requests initial API availability with priority focus on:

- United States: Aligned with FTC consumer fraud reporting, the Consumer Financial Protection Bureau's APP fraud guidance, and partnership discussions with major US financial institutions and telecoms carriers.
- Canada: Aligned with the Canadian Anti-Fraud Centre (CAFC), the Competition Bureau's fraud prevention mandate, and Canadian bank fraud teams. Canada and the US share significant cross-border scam activity, making simultaneous deployment strategically important.
- United Kingdom: Aligned with UK Government fraud strategy, the Payment Systems Regulator's APP fraud reimbursement regime, and Action Fraud reform.
- Australia: Aligned with ACCC Scamwatch, the Australian Signals Directorate's national scam centre, and major Australian bank fraud teams already engaged as partners.

Phase 1 activity: sandbox access and technical validation with at least one operator - per country.

Phase 2 — Expansion Markets: 6–18 months starting early next year in 2027

Following successful Phase 1 deployment, Unscammed will expand to:

- South Africa: South Africa experiences significant volumes of both domestic and cross-border mobile phone fraud including 'vishing' and SIM swap fraud. Alignment with the South African Banking Risk Information Centre (SABRIC) and local MNOs.
- India: India is both a major target for scam calls and a significant origination country for international telephone fraud operations. Alignment with TRAI's Do-Not-Disturb framework and the Indian Cybercrime Coordination Centre (I4C).
- New Zealand & Singapore: Secondary expansion targets with strong regulatory alignment and existing GSMA Open Gateway operator engagement.

Phase 3 — Global Scale (18+ months based on Phase 1 and Phase 2 implementation)

Unscammed will pursue broader global expansion as operator support, standards maturity, and commercial readiness develop — leveraging the GSMA Open Gateway's standardised framework to avoid each country's - re-integration cost.

7. Technical Integration Requirements

7.1 Authentication & API Access

- OAuth 2.0 client credentials flow for server-to-server (backend) API calls, consistent with the CAMARA security profile.
- Support for the CAMARA commonalities consent model for third-party access. Note: all Unscammed queries relate to numbers reported to Unscammed by third parties, not device-based authentication flows.
- REST/JSON interfaces consistent with CAMARA API specifications published on GitHub (camaraproject.org).

7.2 Performance & Volume

- Latency: <500ms p95 for synchronous query APIs.
- Availability: 99.9% monthly uptime for production access.
- Sustained throughput: 5,000–50,000 API calls/day at launch, scaling to 500,000+ calls/day within 18 months.
- Burst tolerance: 10× sustained rate to accommodate sudden scam campaign spikes affecting a common number range.

7.3 Subscription & Event Delivery

- Reliable webhook delivery for SIM Swap Subscriptions with at-least-once semantics.
- Support for a minimum of 10,000 concurrent active subscriptions at launch.
- Event delivery within 60 seconds of the underlying network event.

8. Data Governance & Compliance Commitments

- Purpose limitation: All API data will be used exclusively for scam detection, threat intelligence production, and consumer protection. No API data will be used for marketing or profiling of non-reported individuals.
- Data minimisation: Unscammed will query only the specific APIs and specific numbers required for active threat intelligence operations.
- Retention: Raw API response data retained for no longer than 12 months. Derived intelligence signals retained for the duration of that number's active status in the threat database.

- Security: API credentials and response data stored with AES-256 encryption at rest and TLS 1.3 in transit. Access restricted to Unscammed staff on a least-privilege basis.
- Regulatory compliance: Unscammed - operates under US state and federal privacy law, Canada's PIPEDA, UK GDPR and the Data Protection Act 2018, the Australian Privacy Act 1988, South Africa's POPIA, and India's DPDP Act 2023, and will comply with applicable privacy regulations in each jurisdiction where it queries operator data.
- Third-party disclosure: Intelligence derived from API data is shared with partner organisations in aggregated or scored form only. Raw telco data is never onward disclosed.
- Consent framework: Unscammed acknowledges that CAMARA API access operates under each operator's identity and consent management framework and is prepared to negotiate bilateral agreements where operator consent regimes require specific contractual arrangements.

9. Call to Action for Mobile Network Operators

Unscammed calls on mobile network operators participating in the GSMA Open Gateway programme to:

- Where available expose fraud prevention APIs as set out in Section 5 of this document, conforming to CAMARA API specifications.
- Target SLAs aligned with latency and availability SLAs suitable for real-time payment and account security decisioning (see Section 7).
- Enable near-term pilots in the United States, Canada, United Kingdom, and Australia where Unscammed can deploy services, validate technical integration, and demonstrate measurable consumer protection outcomes.
- Engage on intelligence reciprocity: Unscammed is prepared to share aggregated, anonymised threat intelligence — including device-level scam patterns, recycled number abuse trends, and call forwarding misuse data — back to participating operators, enhancing their own network integrity programmes.

10. Collaboration & Next Steps

Unscammed supports the GSMA Open Gateway initiative and welcomes collaboration with mobile network operators, channel partners, CAMARA and GSMA Fusion with enterprises, and ecosystem contributors to accelerate deployment of standardised fraud prevention APIs.

We are seeking partners to collaborate on:

- Technical implementation and sandbox access
- Interoperability validation across operator networks
- Commercial model alignment for fraud-prevention API use cases
- Joint pilots with at least one operator in United States, Canada, United Kingdom, Australia, South Africa, and India- with a financial services partner.
- Cross-industry working groups on scam - and threat intelligence sharing frameworks.

We are committed to participating in pilot, live tests and joint industry initiatives to ensure the successful adoption of standardised network APIs at global scale. -

11. Conclusion

Phone-based fraud is one of the fastest-growing consumer harms in the markets Unscammed serves. The phone number is the primary attack vector — and the mobile network operator community uniquely holds the network-level signals that can disrupt it. CAMARA APIs, delivered through the GSMA Open Gateway initiative, represent the most direct and scalable path to making those signals available for consumer protection platforms like Unscammed.

Unscammed is ready to enter in discussions with GSMA Open Gateway, participating operators, and channel partners to progress network API access. We bring an active, rapidly growing threat intelligence database, established partnerships with financial institutions and consumer protection bodies across the United States, Canada, United Kingdom, Australia, South Africa, and India, and a clear, compliance-led operating model for responsible use of operator data.

Together, we can move the industry from reactive fraud recovery to proactive scam prevention — at the network level, in real time, and at global scale.