



D8 Corporation calls on Mobile Network Operators to enable Real-Time Fraud Prevention and Customer Verification for Financial Institutions

Published: 9 Jul 2026

Submitted by: D8 Corporation

Product Focus: Stronghold™ Fraud & AML Platform

Required APIs: SIM Swap, Number Verification, KYC Match, Device Location Verification, Device Roaming Status and Device Identifier

Industry vertical: Financial services (banks, PSPs, fintechs, e-money institutions)

Executive Summary

D8 Corporation provides enterprise-grade fraud prevention, AML, and risk management solutions to regulated financial institutions across multiple international markets.

Our core solution, Stronghold™, provides unified fraud prevention, transaction monitoring, customer verification, and AML capabilities supporting banks, fintechs, payment service providers (PSPs), and electronic money institutions.

Stronghold™ enables organisations to monitor transaction activity in real time, identify anomalous or suspicious behaviour, apply contextual risk scoring, and support customer verification and AML workflows through a single operational environment.

As financial crime vectors continue to evolve, institutions increasingly require trusted, real-time intelligence beyond traditional banking telemetry to improve customer verification and transaction risk assessment. This is particularly relevant in areas such as authorised push payment (APP) fraud, social engineering attacks, account takeover, SIM swap abuse, synthetic identity fraud, and mule account activity.

Mobile Network Operators (MNOs) hold authoritative network-derived customer and device intelligence that can materially improve fraud prevention outcomes when exposed securely through standardised APIs.

D8 Corporation therefore strongly supports the GSMA Open Gateway initiative and requests broader availability of standardised network APIs that can be integrated into the Stronghold™ real-time fraud and AML ecosystem.

Industry Challenge: The Velocity of Real-Time Fraud

The global shift toward instant payment networks such as SEPA Instant, Pix, and FedNow has compressed fraud detection windows from days to milliseconds. At the same time, regulatory expectations continue to intensify, with frameworks such as the UK’s mandatory APP fraud reimbursement requirements shifting increasing financial liability onto financial institutions.

Traditional fraud controls face a critical limitation: they cannot always validate out-of-band context. When social engineering manipulates a legitimate customer, or a compromised device is used to initiate transactions, banking telemetry alone may still appear consistent with normal customer behaviour.

Financial institutions increasingly require additional trusted, real-time signals to strengthen fraud decisioning without introducing unnecessary friction into legitimate customer journeys. While advanced fraud prevention infrastructure has matured significantly across some established banking markets, many rapidly digitising and mobile-first financial markets continue to face growing fraud exposure alongside more limited access to large-scale risk infrastructure, external identity data, and operational fraud resources.

In these environments, mobile network intelligence can provide an especially valuable and scalable trust signal, helping institutions strengthen customer verification and fraud prevention without requiring a complex or cost-prohibitive infrastructure programme.

The Missing Trust Layer: Mobile Network Intelligence in Financial Services

Integrating Open Gateway APIs into Stronghold™ introduces an additional network-verified trust layer into digital financial services workflows. Network-derived signals can help financial institutions:

- identify compromised or recently changed mobile identities,
- validate customer-device relationships,
- strengthen authentication processes,
- detect anomalies associated with fraud,
- validate customer onboarding data,
- and improve confidence during high-risk payment events.

Open Gateway APIs help financial institutions apply stronger risk-based controls while maintaining efficiency and customer experience. Combined with scalable fraud and AML platforms, mobile network intelligence can improve risk scoring, strengthen fraud detection, and support safer digital financial services without major infrastructure change.

Network API Requirements and Expected Benefits

API requirements	Expected Benefits
------------------	-------------------

1. SIM Swap API	Reducing account takeover exposure and social engineering fraud through improved visibility into compromised or recently altered mobile identities.
2. Number Verification API	Improved authentication confidence, reduced onboarding friction, and stronger protection against impersonation and identity misuse.
3. KYC Match API	Improved confidence in digital onboarding processes and reduced exposure to synthetic identity fraud and mule account activity.
4. Device Location Verification API	Improved fraud detection accuracy and reduced false-positive transaction declines
5. Device Roaming Status API	Improved detection of social engineering scenarios, account compromise activity, and anomalous digital session behaviour
6. Device Identifier APIs	High-assurance, -device level verification by linking a user to a trusted physical device, reducing fraud while minimising customer friction

Geographic API Requirements & Priorities

D8 Corporation sees continued demand for Open Gateway-enabled fraud prevention capabilities across both established banking markets and rapidly evolving digital financial ecosystems.

High Priority Markets - These are markets where we already support customers and where early availability of Open Gateway APIs would enable D8 and its customers to evaluate and adopt network intelligence capabilities.

Countries	Primary Drivers
United Kingdom	APP fraud prevention, transaction monitoring, and advanced digital banking protection
Armenia & Georgia	Mobile-first financial services, onboarding security, and AML modernisation
Latvia, Estonia & Lithuania	Cross-border payments, transaction monitoring, and digital banking infrastructure
Uzbekistan & Kyrgyzstan	Rapid fintech expansion, transaction monitoring, AML modernisation, and alternative payment ecosystem growth
Ukraine	Secure digital banking, transaction monitoring, and fraud prevention resilience
Egypt	Mobile banking growth, onboarding protection, and AML modernisation

Medium Priority Markets - We also see growing demand across several additional markets and regions where digital financial ecosystems, mobile payments, and real-time transaction services are expanding rapidly. These markets are characterised by growing digital adoption, increasing fraud and AML requirements, and a rising need for trusted customer verification capabilities. These include MENA markets such as UAE, Jordan, Saudi Arabia, and wider Gulf states; Sub-Saharan African markets including Kenya, Uganda, Tanzania, Ethiopia, and Rwanda; and LATAM markets including Argentina, Chile, Uruguay, Peru, and Ecuador.

Additional markets are expected to emerge as Open Gateway adoption expands globally.

Call to Action and Collaboration

D8 Corporation is calling on mobile network operators to:

- expose standardised Open Gateway fraud and identity related APIs
- support interoperable implementations across markets - this is essential because financial institutions and fraud platforms operate across multiple countries and operators. Without consistent API behaviour and broader market availability, adoption becomes fragmented, integration costs rise, and the fraud prevention value is weakened. Strong ecosystem collaboration is therefore critical to deliver scalable, trusted, and technically viable solutions
- enable commercial accessibility for financial institutions
- participate in pilots focused on real-world fraud prevention outcomes

D8 Corporation invites mobile network operators, GSMA Open Gateway initiative participants, financial institutions, and ecosystem partners to collaborate on expanding the availability of trusted, standardised network intelligence APIs for fraud prevention and customer verification. As digital finance grows, closer collaboration between operators, GSMA, and financial institutions can strengthen trust, reduce fraud, and improve the resilience of digital payments. The following timelines are indicative and will depend on operator readiness and API availability.

- Within the first 6 months, collaboration should focus on technical discovery, sandbox testing, and validation of priority APIs in real fraud and customer verification scenarios. This phase should establish data availability, response quality, workflow fit, and initial success criteria for pilot readiness.
- Between 6 and 12 months, the focus should move to controlled pilot deployments with selected financial institutions and operator partners, including live workflow testing, model and rule validation, performance benchmarking, and production readiness discussions. During this period, partners should also define service levels, support processes, escalation paths, and implementation requirements for scaled adoption.
- Following a successful pilot, collaborators can jointly assess measurable fraud reduction, customer experience impact, operational feasibility, and define a roadmap for broader deployment and market expansion.
- Within 1 to 2 years, successful pilots should transition into production deployment with agreed SLAs, operational governance, monitoring, reporting, and integration into standard fraud and customer verification journeys. This phase should support multi-market expansion, stronger interoperability, and broader commercial availability of network APIs across the financial services ecosystem.

By working together with us, operators, GSMA, and financial institutions can broaden access to stronger fraud prevention through trusted mobile network intelligence and interoperable API frameworks. D8 Corporation believes that direct engagement and ecosystem collaboration can accelerate the adoption of stronger fraud prevention and customer verification capabilities across a broader range of financial markets.

About D8 Corporation

D8 Corporation provides fraud prevention, AML, payment processing, and financial technology solutions for banks, payment service providers, fintechs, and regulated financial institutions across multiple international markets.

Stronghold™ delivers enterprise-grade transaction monitoring, fraud prevention, and risk management capabilities designed to support increasingly real-time, high-volume, and digitally connected financial ecosystems. The solution combines high-performance real-time decisioning with machine learning and AI-assisted operational capabilities that help institutions respond more rapidly to evolving fraud threats, improve detection quality, and reduce operational dependency and time-to-response for new fraud scenarios.

Additionally, with the recent launch of Voora.ai, D8 is extending proven Stronghold™ fraud and AML capabilities into a scalable SaaS delivery model designed to make enterprise-grade fraud prevention, transaction monitoring, and customer verification more accessible across a broader range of financial institutions and markets.