www.pipelinepub.com
Volume 22, Issue 1

Why a National Platform is Necessary to Protect Communication Channels from Fraud

By: Dmitry Sumin

National regulators, charged with consumer protection as well as national security objectives, are becoming more active in the fight against voice and SMS fraud. But legislation on its own has limits.

Operators deploy solutions ranging from number validation to advanced AI-based fraud detection, yet without cooperation across networks, even the most sophisticated tools cannot address the central problem: spoofing.

By promoting technical solutions at the national level, regulators can enable cooperation among operators, enterprises, and government agencies to safeguard the integrity of voice and SMS traffic.

Fraud has gone from nuisance to crisis

Voice and SMS fraud has shifted from an irritating nuisance to a global crisis. Consumers are bombarded with vishing and smishing attempts that cause not only financial losses but also lasting damage to trust in telecom services. Fraud prevention is often framed as an industry problem, but the economic impacts reach much further. Information security is a critical element of national security, and governments are increasingly focused on securing these communication channels.

Consumer scams result in billions of dollars in direct losses every year. In the United States alone, the Federal Trade Commission reported that impersonation scams cost consumers over $1.1 billion in 2023. Similar figures appear in Europe and Asia, where consumers are increasingly targeted by smishing and vishing attacks. These losses translate into reduced consumer confidence and greater demand for regulatory intervention.

Enterprises also suffer: impersonation fraud undermines customer confidence in their brands, while employees and systems are targeted by increasingly sophisticated scams. Over time,

subscribers begin to disengage from voice and SMS altogether, weakening essential communication channels.

National Security - The Cost of Doing Nothing

The consequences of vishing and smishing are not confined to individuals or businesses. Misinformation campaigns during elections and other sensitive events highlight the national security dimension of telecom fraud. When fraudulent communications have political aims, the effects extend to the integrity of democratic processes and public institutions.

Governments also bear indirect costs. Fraud cases drive up spending on law enforcement investigations, court proceedings, and consumer redress. Lost tax revenues from bypass fraud and SIM box schemes further erode national income, diverting resources from other priorities. When consumers lose trust and enterprises disengage from voice and SMS, governments also lose valuable communication channels for public services and security alerts.

Why Spoofing Defeats Traditional Defenses

Spoofing—the manipulation of caller or sender IDs to impersonate a trusted source—is a powerful enabler of telecom fraud. It gives legitimacy to scam calls and smishing attempts, and also underpins many wholesale and interconnect fraud types.

Traditional defenses such as firewalls and fraud management systems rarely detect spoofing reliably. Unless the call or message is flagged for other reasons through content analysis, volumetric thresholds, or anomaly detection, it is likely to reach the end user.

In order to effectively detect spoofing, operators must be able to verify that traffic from numbers belonging to other national operators is valid, whether the traffic originates locally or internationally.

Spoofing also distorts operator economics. Fraudsters use caller ID manipulation to bypass approved routes and mask the true origin of calls, allowing them to exploit interconnect agreements. While frauds that utilize CLI spoofing techniques such as Wangiri, CLI refiling and OBR traffic manipulation may account for a small percentage of total volume, the financial incentives to detect spoofed traffic are significant.

The GSMA has recommended “roaming checks” as a basic control—verifying whether calls from local numbers truly originate abroad when a subscriber is roaming. Yet this simple measure is difficult to implement without real-time verification across networks. And in competitive markets, there is little incentive for operators to share the data required to make it work. This is where regulators have a role to play.

National and Global Lessons in Fraud Prevention

Some regulators have already taken steps to address telecom fraud, though results have been mixed. The most cited example is the FCC’s rollout of STIR/SHAKEN, a protocol designed to authenticate caller IDs in IP-based voice traffic. While the program has had a measurable impact in reducing certain types of robocalls, it has also revealed clear limitations. The authentication protocol does not extend to 2G/3G voice or SMS, is difficult to enforce across international traffic, and has faced adoption challenges among smaller operators. Implementation costs were also significant, and enforcement remains uneven. For these reasons, STIR/SHAKEN is unlikely to be applied at scale outside North America. Other initiatives, such as Do Not Originate (DNO) lists, Do Not Call (DNC) registries, and verified

sender databases, have demonstrated the value of national approaches. Each tackles a narrow aspect of the problem, but together they underscore an important point: national-level solutions can achieve results that isolated operator efforts cannot.

Some of the most effective examples have come from emerging markets, where regulators implemented national-level SIM box detection or interconnect monitoring platforms. In several African and Central Asian countries, these initiatives have rapidly and drastically reduced bypass fraud. These experiences demonstrate that when regulators provide both the framework and the mandate, cooperation among operators becomes not only possible but highly effective.

More Collaboration, Less Punishment

The question is not whether regulators should act, but how. Punitive measures alone (fines and penalties imposed after violations) have a limited effect. A more promising path lies in enabling centralized, technical solutions that prevent fraud at its source.

Enforcement and compliance remain resource-intensive. When regulators and operators are entrenched in an adversarial relationship, disputes over culpability consume time and legal resources that might otherwise go toward proactive fraud prevention. Unfortunately, models of constructive cooperation between regulators and service providers remain scarce.

Telecom regulators are in a unique position to unite service providers, enterprise, and other government agencies in a common cause, but must also provide technical frameworks for cooperation.

National anti-fraud platforms provide such a framework. By allowing operators to share essential traffic validation data in real time, they make it possible to detect spoofing and other manipulations before they reach end users. Discrepancies between originating and terminating data indicate fraud, enabling operators to block suspicious calls or messages immediately.

At the same time, these platforms give regulators visibility into compliance. Instead of relying on evidence of violations after the fact, regulators can confirm that operators are participating in fraud prevention in real time. In addition, centralized platforms can enforce databases such as DNO, DNC, and verified sender lists consistently across the entire national telecom environment.

An expanded role for regulatory agencies – shifting from punitive regulation to technical collaboration – has the potential to reduce fraud more effectively, while also lowering the administrative burden on both operators and regulators.

Beyond Fraud: Wider Benefits of National Collaboration

The value of a national anti-fraud framework extends far beyond blocking scams and spam. By implementing national platforms, regulators reduce cascading costs. A framework for shared fraud intelligence and real-time validation is more efficient than a patchwork of fines, litigation, and after-the-fact enforcement. Over time, national collaboration saves not only consumer losses but also the operational and enforcement costs borne by regulators themselves.

For governments, a secure telecom environment is part of broader national resilience. Preventing spoofing directly supports election integrity by ensuring that political

disinformation campaigns cannot spread unchecked through automated calls or fraudulent SMS campaigns. Verified communications also make it easier for governments to run official public information campaigns, particularly during crises such as natural disasters or public health emergencies.

For enterprises, national-level protections reduce reputational risk. When customers can trust that messages from their bank, utility provider, or delivery service are authentic, engagement improves and complaints decline.

For consumers, national collaboration translates into fewer fraudulent calls and messages, and renewed confidence in telecom channels that have been steadily eroded by scams and spam. This consumer trust is ultimately what protects the relevance of voice and SMS as reliable communication tools.

When regulators convene stakeholders around shared technical platforms, they do more than stop fraud. They create a framework that reinforces national security, enterprise communication, and consumer protection all at once.

The End of Fraud

Spoofing, scams, spam, and misinformation cannot be eradicated by operators acting alone. Nor can legislation by itself keep pace with evolving fraud tactics. The only sustainable path forward is coordinated collaboration at the national level.

Regulators have a unique opportunity to bring together operators, enterprises, and government stakeholders in a shared framework that addresses fraud proactively. By doing so, they not only protect consumers but also strengthen national security and reinforce confidence in digital communications.

A national anti-fraud platform gives operators the means to collaborate in real time while providing regulators with centralized oversight. At scale, this model represents the most comprehensive approach to protecting consumers, enterprises, and communication service providers from voice and SMS fraud.