Improving Global SMS Routing Security and Efficiency
Addressing the Critical Need for Centralized SMS Sender ID Registries Worldwide

SIPNOC 2024

Text Messaging Landscape

Main Concerns in Text Messaging

Message Trashing

Cost Increase

AIT

Grey routing

Brand Impersonation

Malware

Spoofing

Smishing

SIM farms

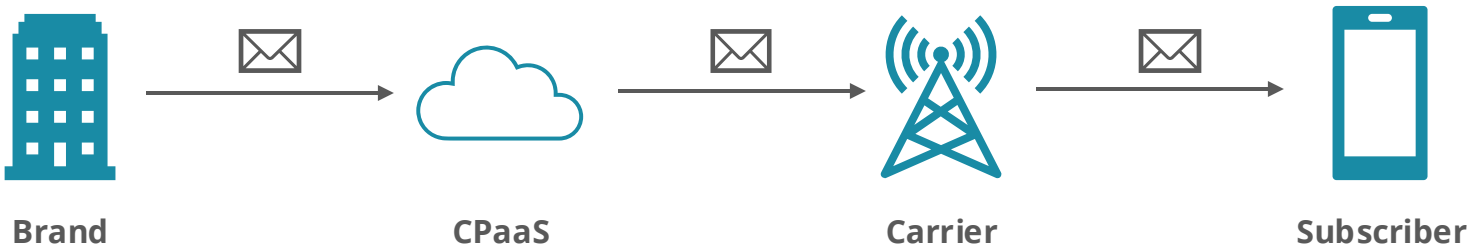
Spam

This Time It‘s Serious

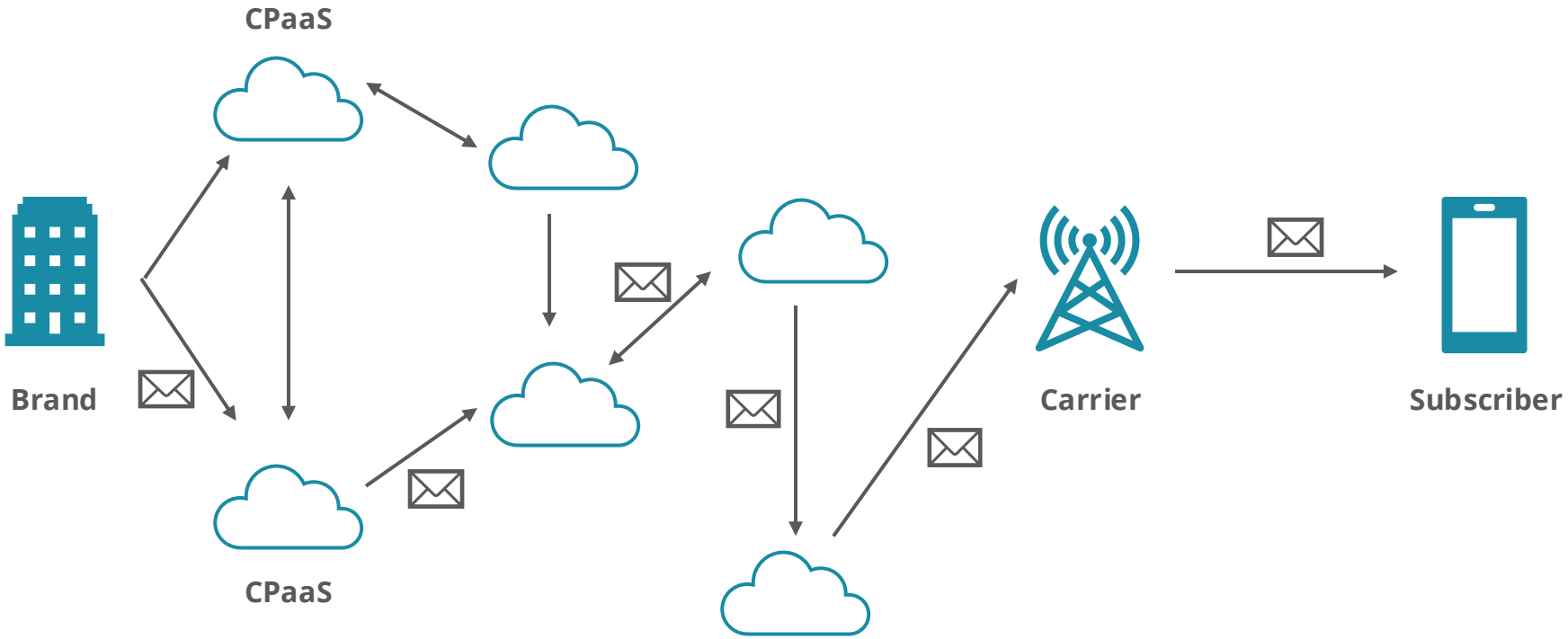
- Almost all markets saw a decline in A2P SMS traffic in 2023 (Mobilesquared, 2024 A2P SMS Pricing Impact Report)
- Alternative channels to A2P SMS are deployed with increased success (carrier APIs, OTT messaging apps)
- Regulators globally dedicate more and more attention to text messaging
    - FCC: Targeting and Eliminating Unlawful Text Messages
    - Singapore: Government-mandated SMS Sender ID Registry
    - Comreg (Ireland): Consultation on Combatting Scam Calls and Texts
    - ACMA (Australia): Sender ID Registry consultation

Text Messaging 101

How A2P SMS Aggregation Works



Just Kidding...



How Did We Get Here?

- **Low cost as primary performance criteria**
  Many brands have prioritized low messaging cost against for years now. Few can measure actual performance accurately by using conversion rate KPIs.
- **Impossible to measure termination performance accurately**
  Delivery receipts are not reliable. Conversion rates can only be measured for call to action.
- **Termination cost increases**
  Many carriers have raised prices, which lead to higher costs for brands.
- **Long SMS delivery chains (many hops)**
  This reduces transparency and accountability
- **Brands often approach SMS like email...**
  ... and are not expecting the myriad of fraud methods common in SMS.

Key Issue: Sender ID Spoofing

- In most countries, there are **no regulations or even common guidelines** on the use of sender IDs
- Carrier sender ID requirements for sender IDs vary:
  - Supported sender ID types (alphanumeric, short code, long code)
  - Registration process (required or not, who can register a sender ID)
- The SMS protocols allow virtually **any sender ID to be freely set by the sender**
- To circumvent sender ID registration requirements, **“generic” sender IDs** are used, e.g. “Verify”
- Sender ID spoofing is not just “nuisance” but the **entry door for fraud**: spam, smishing, brand impersonation, AIT, grey routing / SIM farms, malware

Sender ID Protection

Why Sender ID Registration Matters

- Sender ID Registration is the foundation of authentication in text messaging
- If the identity of the sender can be trusted, some types of fraud can be significantly reduced
- Content protection and URL screening is cumbersome, but adds a much-needed layer
- Sender creativity needs to be tackled – for example ‘SINCH’ could be locked & ‘SlNCH’ wide open

Markets with strict sender ID registries have virtually no spoofing issues. In the US, where the nnSR acts as the sender ID registry, the FCC has acknowledged that spoofing is ”rare”. Singapore is another example of a country with a compulsory sender ID registry mandated by the government.

Low

High

Protection

No Registration

- No requirement to register sender IDs
- Carriers might still limit sender ID use by type (e.g., allow alphanumeric and short code but not long code)

Pros:

- No cost with managing a registry and the registration processes

Cons:

- The door is wide-open to abuse based on spoofing

Registration by the Carrier

- Attempt to control sender ID allocation at carrier level
- Messaging providers with direct relationships to the carrier submit sender ID registration via manual processes (emails or forms)

Pros:

- Adds some protection for the specific carrier's subscriber base
- Better than nothing

Cons:

- Highly manual process. Prone to errors and inconsistencies. Slow and dependent on firewall implementation/management
- Impossible to truly control sender ID allocation. Messaging providers claim to serve specific brands, but they might just be intermediaries in a long delivery chain.

Optional Sender ID Registries

- Industry-led initiatives to create “whitelists” of sender IDs, i.e., lists of sender IDs claimed by brands and the messaging providers that should be allowed to carry traffic with those sender IDs.
- There is no requirement for anyone in the delivery chain to actually use those registries.

Pros:

- Centralized sender ID information, centralized processes.

Cons:

- Typically manual processes. Prone to errors and inconsistencies. Slow.
- Impossible to enforce any rules across the ecosystem. Messaging providers can carry traffic without observing the registry rules.

Low

High

Protection

Strict Sender ID Registries

- Centralized sender ID registries with vetting, access rights control and conflict resolution
- Well defined roles (brand, CPaaS, carrier) and processes
- The entire ecosystem in the respective countries agrees voluntarily or is mandated by the regulator to use the registry

Pros:

- Ensures fair and verified sender ID allocation to brands and their messaging providers.
- Central source of truth that the ecosystem leverages to ensure optimal processes

Cons:

- Takes longer to set up, but once it's up and running, it increases the efficiency and the security of the messaging ecosystem in the respective country.
- Done incorrectly, could seriously hamper both new and existing business

Takeaways

Takeaways

- Poor sender ID registration frameworks are an enabler of nuisance and fraud
- Most of today’s sender ID registration frameworks are neither effective nor efficient (i.e., those which are carrier-led or the optional registries)
- A strict national sender ID registry is essential to ensure vetted access to the messaging ecosystem, fair sender ID allocation and legitimate use. It further protects all industry participants from fraud connected with sender ID spoofing.
- Make it easy to do the right thing
- Enforce consequences for parties that won't play ball

Thank you!