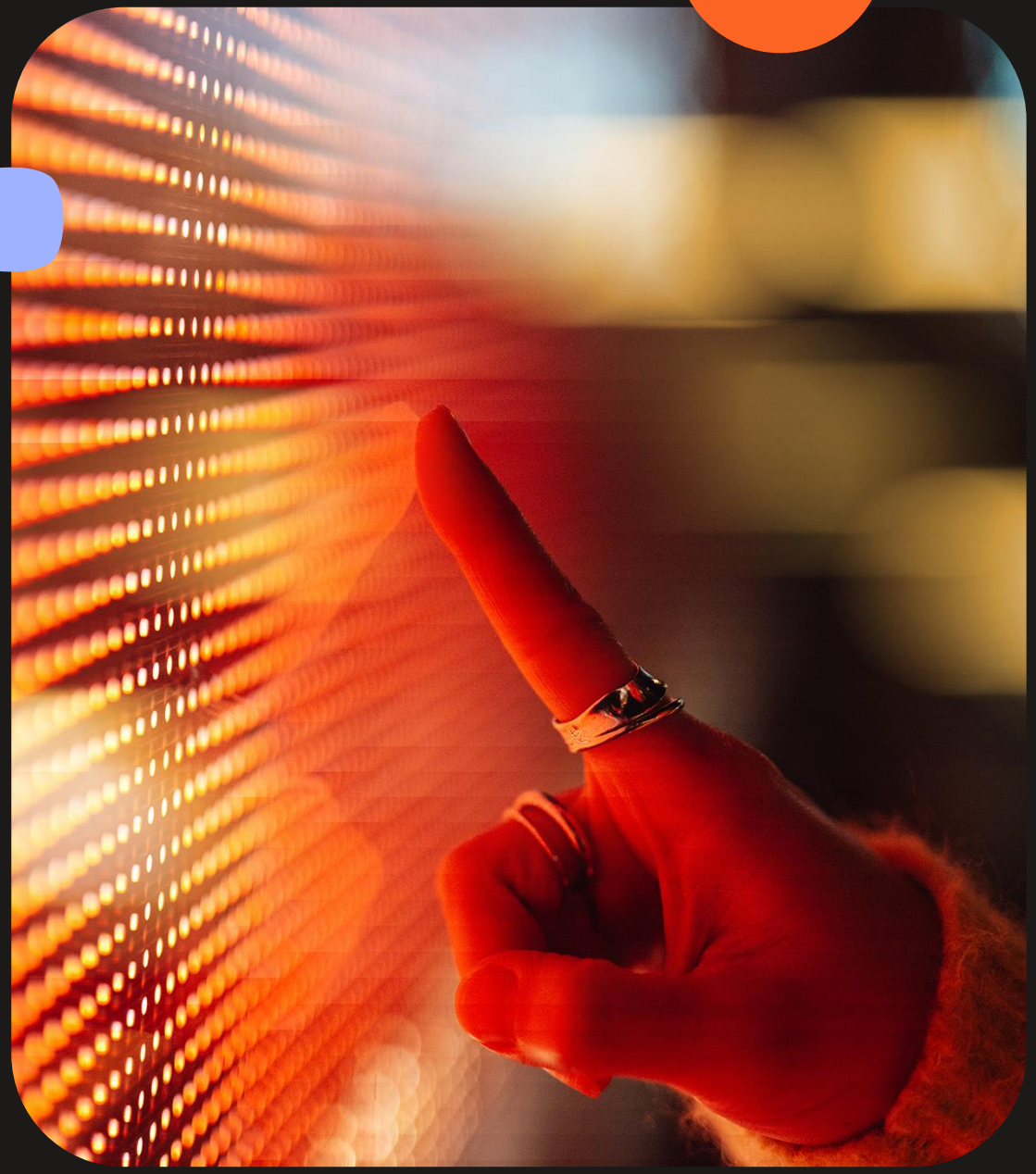
infobip

Securing Messaging Ecosystems in the Era of Relentless Fraud

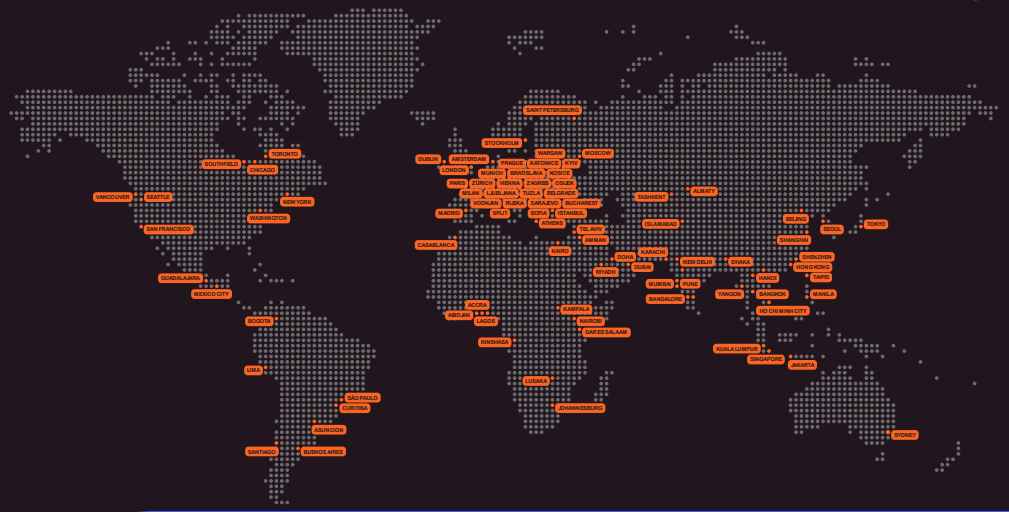
Why Complacency Is No Longer an Option



MAY 2025

#1 Global Cloud Communications Platform, trusted by global brands and world's most disruptive companies

GLOBAL FOOTPRINT



STELLAR GLOBAL CLIENT BASE

Walmart · Dior · PHILIPS
Coca-Cola · NISSAN · daraz · SAMSUNG
unicef · LG · amazon
COSTCO WHOLESALE · ccc · NIVEA
Unilever · BURGER KING · e& · KFC

TELECOM CUSTOMERS

T · orange · vodafone
Telefónica · TELE2 · Claro
Digicel · Jazz · indosat OOREDOO HUTCHISON
Virgin media O2 · vivo · zain
MTN · Smart · truemove

65+
Integration Partners
Extensive Marketplace

75+
Offices on 6 continents
Global reach >190 countries

3.6K+
Employees globally
Global presence, local reach

40+
Data Centers globally
Scalable infrastructure

800+
Direct operator connections
Largest global MNO network

42 Bn+
Monthly interactions
Infrastructure to handle vast volume

80k+
Black Friday Record
Transactions per Second.

2.36 Bn+
Interactions in one day on Black Friday
#wearejuststarting

Introduction: Current Fraud Volumes

- Global: fraud causes losses > $38.95 billion annually
  - 2.5% of telecom industry revenues
- In 2022, Belgium reported €39.8 million in phishing-related losses
  - **+60% vs. 2021**
- Ireland lost €115 million to SMS fraud.
- In the first month of the COVID pandemic, EU-wide phishing attacks soared by 667%.

MESSAGING ECOSYSTEM

Impact of Fraudulent SMS

01

Subscribers

- Exposed to identity theft, phishing, financial loss, and invasion of privacy.
- Smishing attacks erode trust in mobile communications and frequently result in direct financial harm.

02

Mobile Network Operators

- Suffer reputational damage and diminished customer trust.
- Experience revenue leakage and increased costs in fraud handling, customer support, and regulatory compliance.
- Vulnerable to penalties or disputes arising from unchecked fraud in their network.

03

Enterprises

- Face business interruption, financial losses, and damage to brand reputation.
- Authentic enterprise messages risk being distrusted or ignored by consumers due to the prevalence of fraudulent SMS.
- Increased operational costs in fraud monitoring, incident response, and customer remediation.

Regulatory Challenges

Barriers to Fraud Prevention

- Member States shall ensure the confidentiality of communications and shall prohibit interception of communications (Article 5)

ePrivacy Directive vs NIS2

- Operators must take appropriate measures to manage the risks posed to the security of network, systems and recipients of their services (Article 21)
  - *The only appropriate measure to manage the risk from fraudulent SMS traffic is content filtering solution/firewalls*

- NIS2 support content filtering aim at user and infrastructure security
- National adoption is inconsistent and slow
  - Ambiguous local interpretations of confidentiality rules
  - Lack of harmonized legal frameworks to enable fully automated detection and blocking of SMS threats.
- National laws (e.g. Poland) already recognize and permit active content analysis to prevent fraud

Barriers to Fraud Prevention

- EUROPEAN COMMISSION'S NIS2 IMPLEMENTING REGULATION 2024/2690 of 17 October 2024:
  - "*The relevant entities should deploy email filters to reduce exposure to malicious content*"
- Email and SMS are both subject to ePrivacy rules; SMS filters should be treated like email filters

Email providers use extensive filtering, while at the same time SMS systems are bound by strict privacy interpretation

- EU operators are reluctant to deploy SMS filters even though it is the only effective and appropriate measure against SMS fraud
- This hesitation is due to the high fines associated with non-compliance with the ePrivacy Directive
- However, under the NIS2 Directive, mobile operators are required to protect their users from such fraudulent SMS traffic

Mature Telecom Security Solutions Exist—Clearer Legislation Needed

- Advanced, market-tested solutions (like SMS firewalls, content filtering, and AI-driven fraud detection) are already available, made within the EU and widely deployed globally to mitigate SMS and messaging fraud.
- ENISA recommends the implementation of such solutions to achieve robust, harmonized telecom security across Member States (ENISA Threat Landscape 2020 – Spam).
- Despite EU-level rules (NIS2), fragmented and sometimes ambiguous local (national) legislation continues to hinder the full deployment of effective filtering and prevention technologies.
- Poland provides a strong regulatory blueprint: Its legislation expressly enables telecom operators to automatically analyze and filter SMS content to prevent threats (smishing, spoofing, malware) while balancing user privacy and network security
- Recommendation: Major effort is needed to harmonize and clarify EU and national laws, looking to Polish best practice - **explicitly permitting content filtering for telecom security** - as a model for effective and safe fraud prevention.

Thank you

Filip Filković

Telecom Business Director

filip.filkovic@infobip.com

www.infobip.com

Martino Pekas

Counsel

martino.pekas@infobip.com