AB HANDSHAKE

FRAUD REPORT

Q1 2026

ABHANDSHAKE.COM

Q1 2026 FRAUD REPORT BY AB HANDSHAKE

This report pulls together our quarterly findings, explains what each fraud looks like in practice, shares real-world patterns and anecdotes, and closes with practical detection and mitigation advice driven by AB Handshake's AI-equipped Fraud Management System.

Telecom fraud never stops; it only changes. Q1 2026 was full of surprising events across our customer base and the traffic we are deployed on, as fraudulent attacks continue attempting to break through defences.

Our Q1 2026 review focuses on the major fraud vectors observed in voice and SMS traffic monitored by AB Handshake Fraud Management System:

THE AB HANDSHAKE SYSTEM – REPORT DATA SOURCE

AB Handshake has created a global system of products and solutions designed to eliminate all forms of voice and SMS fraud.

Altogether, AB Handshake's solutions process over 200 million call attempts daily for more than 160 operators each month.

This report is based on anonymized statistics from AB Handshake's machine learning-powered AI Shield solution, which detects and blocks voice and SMS fraud in real time with an industry-leading accuracy of 99.995 %, < 0.001% false positive rate, and a false discovery rate of < 3%.

This report summarizes all fraud cases detected by AI Shield. All data has been reviewed by the AB Handshake analytical team, visualized and prepared for this report in accordance with data protection policy.

THE REPORT INCLUDES INFORMATION ON A SELECTION OF THE FOLLOWING FRAUD TYPES:

IRSF

International Revenue Share Fraud (IRSF). A type of voice fraud that involves the artificial inflation of a revenue share number that the fraudster will gain profit from. Different fraud methods are used to commit IRSF, and can include PBX Hacking, Wangiri, Wangiri 2.0, P2S fraud, etc.

PBX HACKING

A voice fraud method where fraudsters gain unauthorized access to a business's phone system and typically use it to generate outbound IRSF calls towards revenue share numbers at the victim's expense.

P2S (PIN TO SPEECH) FRAUD

A Wangiri 2.0 fraud scheme scenario. Fraudsters use bots or scripts to stuff an Enterprise`s online form with revenue share numbers, aiming to request one-time passwords (PIN codes). The enterprise then automatically sends these calls to these revenue share numbers which the fraudster will gain revenue from.

WANGIRI

A type of voice fraud where fraudsters make many zero-duration (missed calls) or short duration calls to unknowing subscribers from a revenue share number. The fraudster will gain revenue from those who call back.

WANGIRI 2.0

Fraudsters use bots or scripts to fill out enterprises' online forms with revenue share numbers, to request automatic callbacks either by a robot or an employee.

SPAM

Unsolicited inbound calls to subscribers, including scam calls, nuisance calls or even silent calls. Can be conducted for telemarketing or scam purposes such as from large scale robocallers or unauthroized call centres.

FLASH CALLS

Not considered a fraud scheme but an undesirable traffic type for carriers which seeks replace traditional A2P authenticaion services for one time passwords (OTPs). Flash Calls are zero-duration calls triggered to subscribers who have requested an OTP, where the call's CLI has been manipulated to include the digits of the intended OTP.

AIT SMS

Artificially inflated traffic is a type of fraud where artificial traffic is generated, such as fake requests for one time passwords (OTP's) or fake new user requests that trigger large amounts of one time password A2P messages. These requests cause revenue loss for the Enterprise being targetted, as well as brand and financial distortion to support large amounts of fictitious new users.

IF YOU WOULD LIKE TO RECEIVE REAL-TIME ALERTS FROM US:

Apply

IF YOU WOULD LIKE TO SUBSCRIBE TO OUR WEEKLY REPORTS:

Subscribe

IRSF

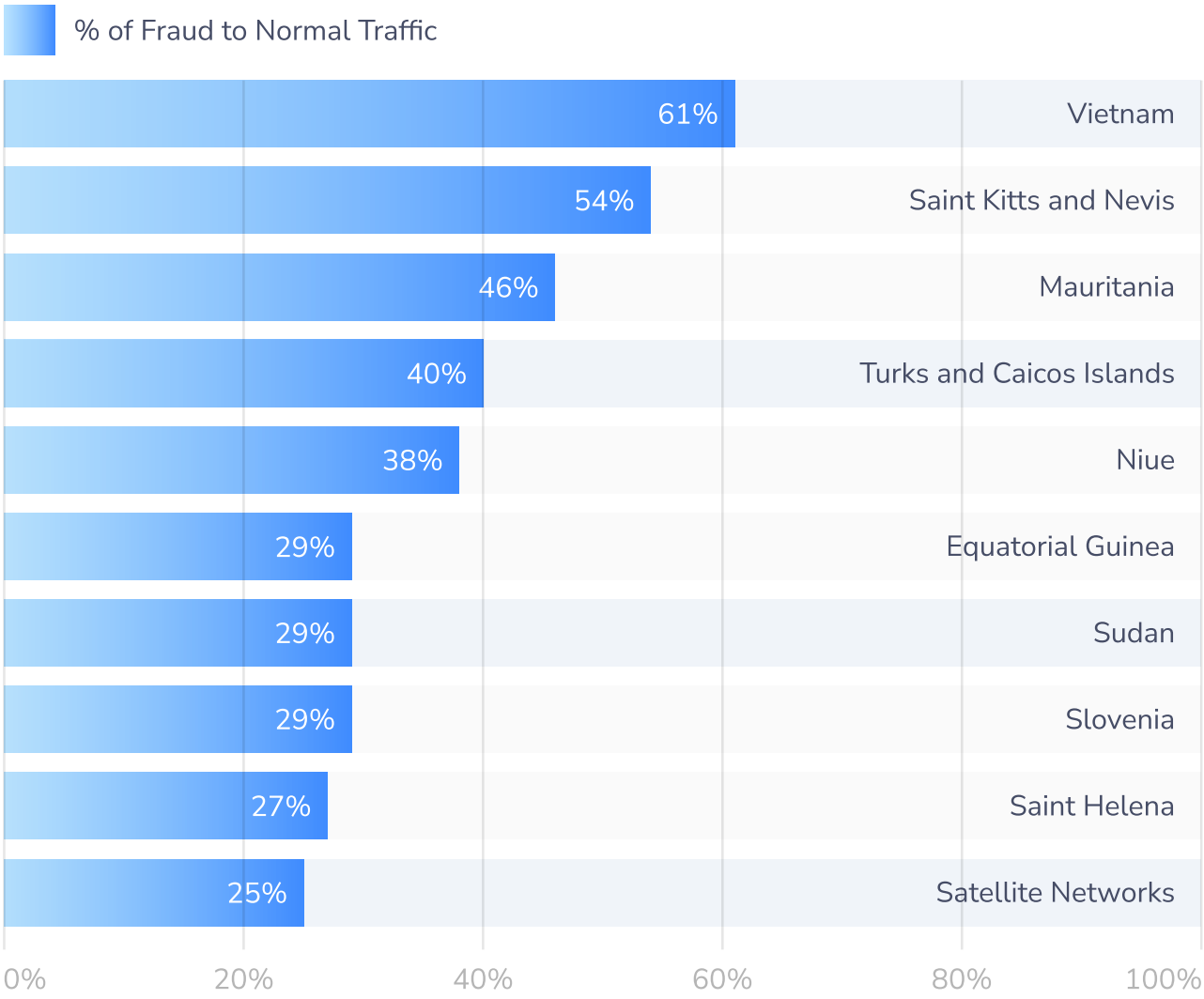
IRSF (International Revenue Share Fraud) typically includes fraudsters artificially driving traffic towards revenue share numbers, from which they gain a profit. IRSF may also occur in combination with other fraud types such as subscription fraud, device theft, roaming events, or PBX hacking.

Q1 2026 HIGHLIGHTS

Top country codes with the highest percentage of IRSF relative to the total traffic terminating to that county code: Vietnam led with a fraud ratio of 61%, followed by Saint Kitts and Nevis at 54%, and Mauritania at 46%.

This section presents the top 10 country range codes where IRSF (International Revenue Share Fraud) traffic had the highest ratio compared to legitimate (normal) traffic.

TOP FRAUD DESTINATIONS - % FRAUD



IRSF TRENDS IN Q1 2026: WHEN HOLIDAY HOTSPOTS BECOME FRAUD HOTSPOTS

The latest Q1 2026 data on International Revenue Share Fraud (IRSF) highlights a familiar but evolving pattern: fraud continues to concentrate in destinations with relatively low volumes of legitimate traffic, but that story is beginning to shift.

Looking at the top fraud destination country ranges this quarter, several expected high-risk regions appear, but what stands out is the presence of number ranges in increasingly popular holiday destinations such as Saint Kitts and Nevis, Turks and Caicos Islands, Niue, and Saint Helena. These are not traditionally high-volume telecom routes, yet they are showing disproportionately high fraud-to-traffic ratios. When legitimate call volumes are typically low, even modest fraud activity can create a highly visible spike. In environments like these, IRSF detection is often straightforward, with basic threshold-based systems able to flag anomalies quickly because the baseline is so low.

The nuance in Q1 2026's data lies in the detail. Many of these locations are growing in popularity as travel destinations, so as tourism increases, so too does legitimate telecom traffic. This creates a blending effect: genuine seasonal spikes (holiday travel, roaming usage, increased international calls) begin to overlap with fraudulent patterns. Right now, that overlap still works in favour of fraud detection. Volumes remain low enough that IRSF activity stands out clearly, and a sudden surge of voice traffic to country ranges like Saint Kitts or Turks and Caicos is still anomalous in most networks.

But this may not hold for long, especially as global travel continues to expand. Over time, the distinction between legitimate and fraudulent traffic will blur, seasonal peaks will become less pronounced, and baseline traffic will rise, reducing the effectiveness of simple rule-based detection. In other words, the very characteristic that makes these destinations easy to monitor today — such as low and stable traffic — is likely to disappear. This is where the industry faces a forward-looking challenge.

Traditional IRSF detection methods rely heavily on static thresholds and historical norms being breached, especially in high-risk destinations. However, in a world where traffic patterns are becoming more dynamic and influenced by external factors like tourism trends, these approaches will struggle to keep pace. AI-driven detection is the solution, offering a path forward by continuously learning traffic behaviours, identifying subtle deviations, and contextualizing anomalies against evolving patterns.

Q1 2026 serves as a reminder: today's easy wins in IRSF detection may become tomorrow's blind spots.

As traffic complexity grows, so does the need for smarter protection, which is why AB Handshake provides AI-powered IRSF detection as a core feature of its voice offering. Operators that adapt early by investing in more intelligent, adaptive detection capabilities will be best positioned to manage this transition.

IRSF – PBX HACKING

UNDERSTANDING IRSF TRAFFIC AND PBX HACKING METHODS

IRSF (International Revenue Share Fraud) typically includes fraudsters artificially driving traffic towards revenue share numbers, from which they gain a profit. IRSF may also often occur in combination with other fraud types such as subscription fraud, device theft, roaming events, or PBX hacking

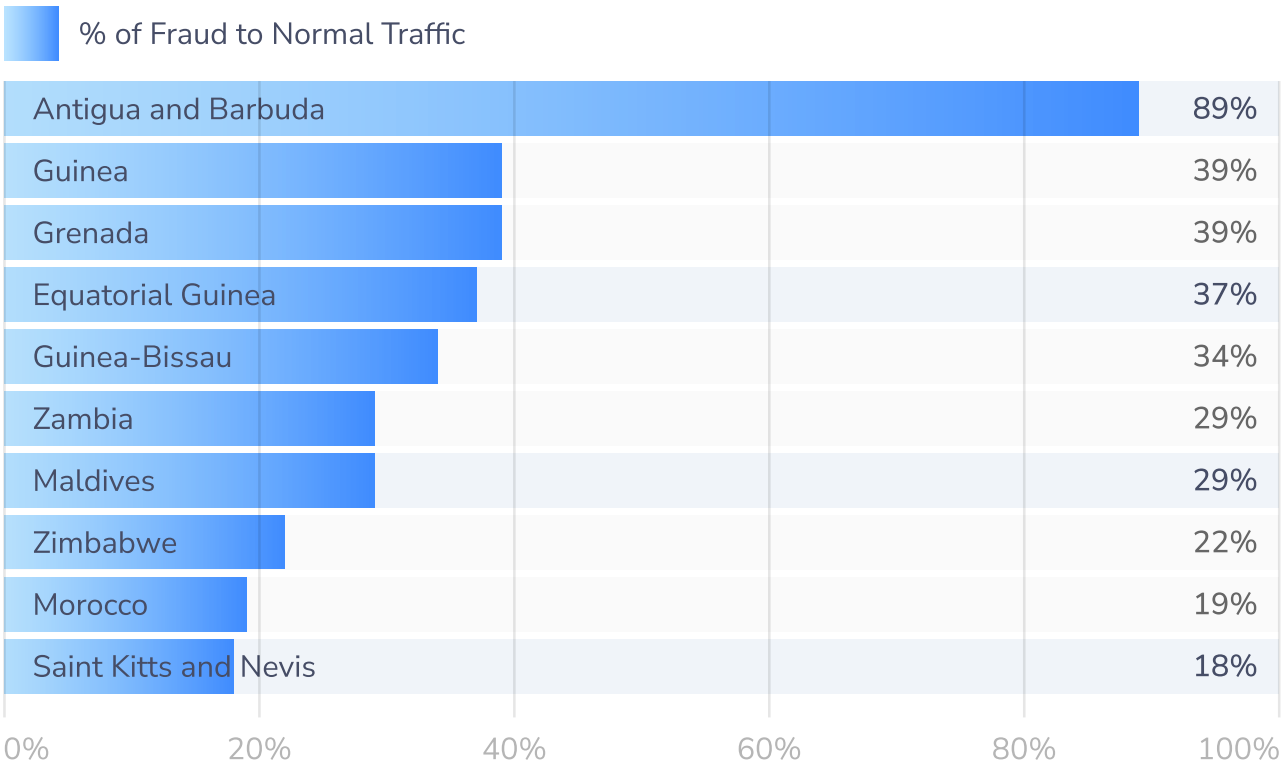
PBX systems are often used as a fraud method to commit IRSF. Fraudsters access badly secured PBX devices within businesses and use them to generate artificial traffic towards revenue share numbers. PBX hacking can be identified within typical IRSF attacks, as calls are often timed in one of two ways depending on the business profile: either for the calls to only occur during business hours (so nobody questions who is making calls during the night), or else to only occur outside of business hours (to ensure employees do not notice constant busy lines during their work day).

Q1 2026 HIGHLIGHTS

Top country codes identified with this traffic type: Antigua and Barbuda recorded the highest ratio at 89%, followed by Guinea at 39% and Grenada at 39%.

The following dashboard identifies the top 10 country ranges where PBX hacking traffic had the highest ratio compared to normal (legitimate) traffic during the quarter.

TOP FRAUD DESTINATIONS - % FRAUD



IRSF – PBX HACKING

ARE FRAUDSTERS EVEN TRYING TO HIDE ANYMORE?

One of the more striking observations from recent IRSF data generated through PBX hacking isn't just "where" fraud is terminating towards, but how predictable those destinations have become. We continue to see the same high-risk country range names appear time and time again. This raises an important question: why aren't fraudsters even attempting to disguise their activity? The answer is simple: they do not need to.

Historically, there has been an assumption that IRSF would evolve toward increasingly sophisticated evasion tactics — that fraudsters would diversify destinations, mimic legitimate traffic patterns, or attempt to blend into normal routing behaviour. However, in practice, much of today's activity suggests the opposite. Fraud is still terminating toward many well-known, well-documented high-risk destination country ranges, and it is still succeeding. This tells us something critical about the current state of detection across the industry.

If traffic to "predictable" IRSF destination country ranges is still being consistently targeted by attackers, it means that basic controls are either not in place, not effective, or not acting quickly enough. In other words, the barrier to executing successful IRSF remains so low that, from a fraudster's perspective, there is no incentive to be clever if simple methods continue to work.

This is particularly evident in automated attack scenarios, where large volumes of traffic can be generated rapidly and directed toward high-yield destinations. These attacks prioritise speed and return over subtlety. The goal is not to remain undetected indefinitely; it is to monetise quickly before intervention occurs. If even short-lived bursts of traffic to well-known destinations can generate value, then sophistication becomes unnecessary.

The implication is clear: IRSF is not just a problem of "detection capability" but of "domain knowledge." It is no longer enough to recognise risky destination ranges or rely on static rules and historical knowledge. By the time a rule is triggered or a threshold is breached, the damage may already be done. What's needed is the ability to identify abnormal behaviour as it happens, regardless of whether the destination is "historically risky," as the real signal is not the destination itself, but the pattern of activity.

Such incidents clearly illustrate the value of deploying an advanced fraud management system like AB Handshake's AI Shield to detect IRSF anomalies and prevent financial exposure.

P2S

UNDERSTANDING P2S

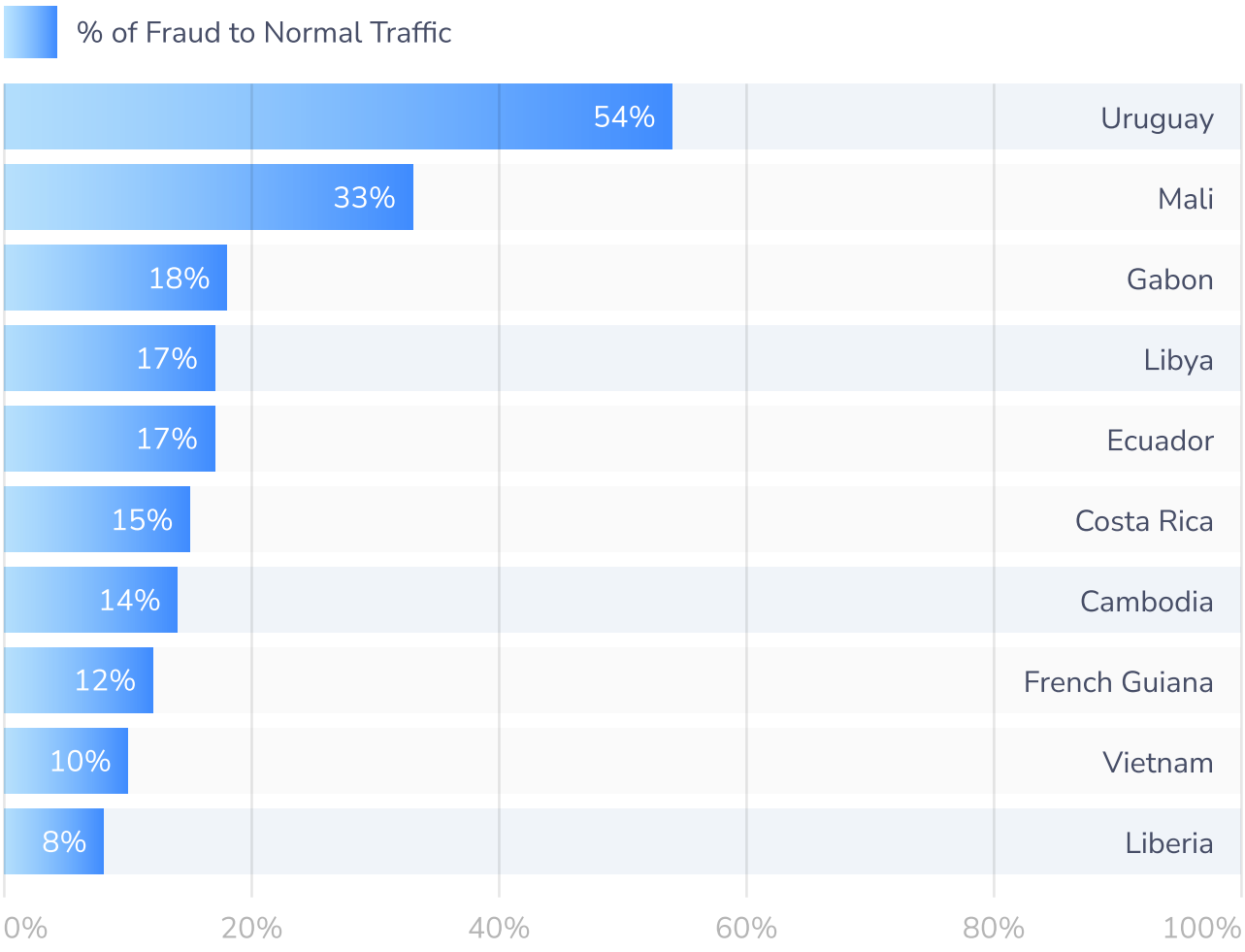
P2S attacks typically involve automated bots or scripts abusing web forms or online verification processes to trigger voice-based OTP calls to revenue share numbers, from which fraudsters gain revenue. Such patterns often reveal systematic P2S attacks, where repeated automated attempts focus on specific destinations, highlighting them as potential hotspots for this type of revenue share fraud.

Q1 2026 HIGHLIGHTS

Top country codes identified with this traffic type: Uruguay recorded the highest ratio at 54%, followed by Mali at 33% and Gabon at 18%.

The following dashboard identifies the country code ranges with the highest levels of P2S fraudulent traffic terminating to them.

TOP FRAUD DESTINATIONS - % FRAUD



P2S

P2S FRAUD IN Q1 2026: WHY ATTACKERS DON'T NEED TO BE SUBTLE

One of the more telling patterns emerging from Q1 2026 IRSF data is how predictable certain destinations remain, even in newer fraud models like P2S attacks. Destinations such as Uruguay and Mali are showing elevated fraud-to-traffic ratios, driven not by traditional call patterns, but by repeated triggering of voice-based OTP calls. These are not random spikes, but instead systematic, automated, and highly targeted — and perhaps most notably, they are not subtle.

P2S attacks typically originate through the online abuse of web forms or verification processes to trigger OTP voice calls to revenue share numbers that fraudsters profit from. Each call generates revenue, and at scale, even short-lived campaigns can be highly profitable. What stands out in the data is that these attacks are not attempting to disguise themselves by distributing traffic widely or mimicking organic behaviour. Instead, they repeatedly target the same revenue share destination ranges. Why? Because they don't need to hide.

Attackers can generate large volumes of traffic quickly, monetise within a short window, and move on. If obvious, repetitive traffic to known high-risk revenue share destination ranges continues to succeed, there is little incentive for attackers to evolve toward more sophisticated evasion techniques — and this is where the real challenge emerges.

From a telecom perspective, the traffic generated by P2S attacks often looks legitimate. OTP calls are expected behaviour: they are system-generated, triggered by user actions (or what appear to be user actions), and typically routed through standard channels. There is no clear "compromise" event and no obvious anomaly in isolation — just a high volume of seemingly valid requests. This creates a critical blind spot.

Traditional detection methods such as static thresholds, destination-based blocking, or rule-based systems struggle in this environment. By the time abnormal volumes are recognised, the traffic has already been delivered and the revenue has already been lost. Patterns such as repetition, velocity, and triggering behaviour across channels become the key indicators of fraud, and these are precisely the types of signals that require continuous, adaptive analysis.

This emphasises the need for intelligent automation in fraud prevention — an area where AB Handshake's AI Shield offers significant operational advantages.

WANGIRI 2.0

UNDERSTANDING WANGIRI 2.0

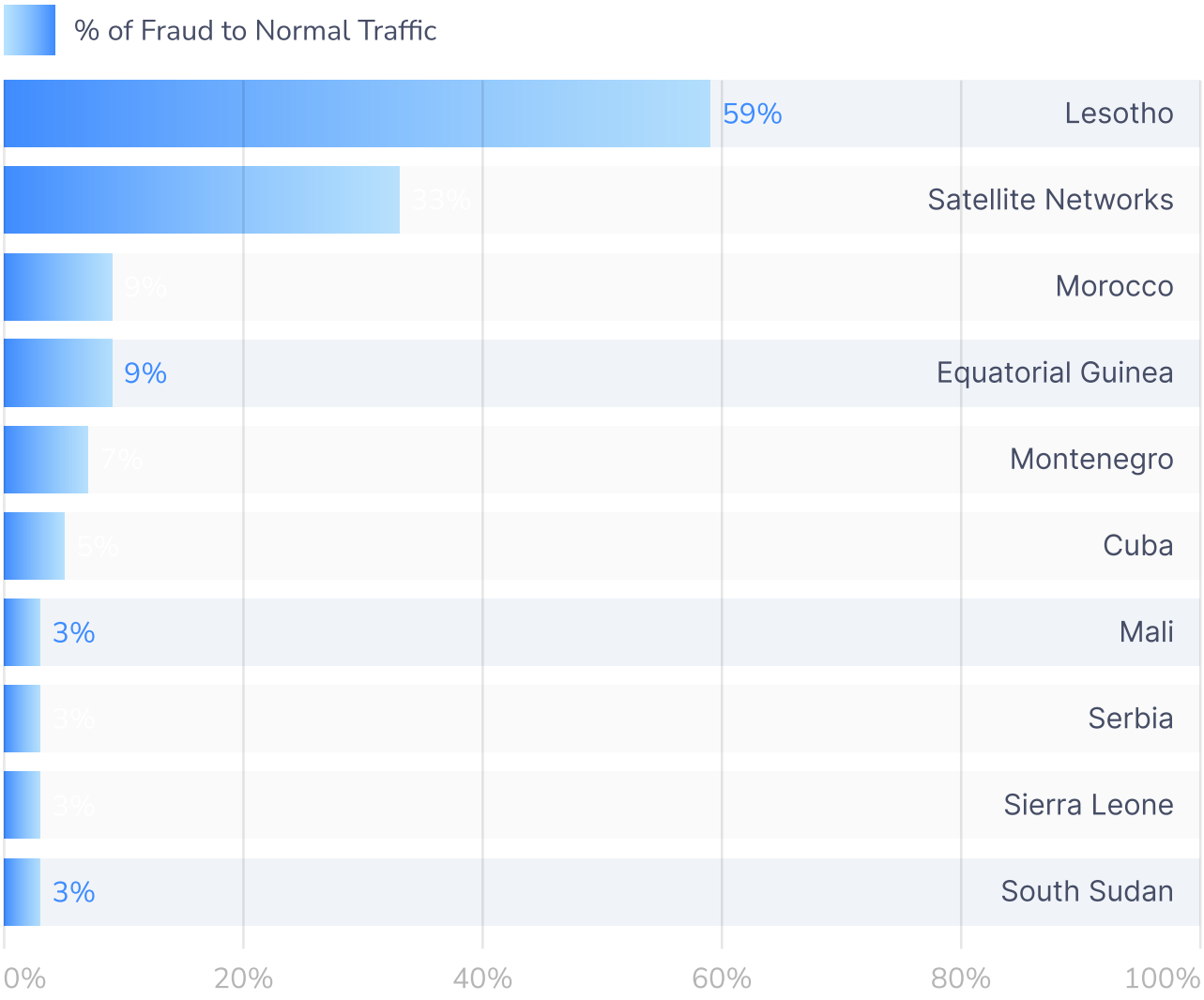
Wangiri 2.0 typically involves automated systems or bots that submit revenue share numbers through online forms, triggering automated callbacks from enterprises or applications.

Q1 2026 HIGHLIGHTS

Top country codes identified with this traffic type: Lesotho recorded the highest ratio at 59%, followed by satellite networks at 33% and Morocco at 9%.

This section displays the top 10 country range codes where Wangiri 2.0 callback fraud made up the largest share of total traffic during the quarter.

TOP FRAUD DESTINATIONS - % FRAUD



WANGIRI 2.0

WANGIRI IN Q1 2026: THE PERSISTENT PULL OF SATELLITE NETWORKS

Among the top Wangiri destinations in Q1 2026, one category continues to stand out: satellite networks. With fraud-to-traffic ratios reaching as high as 33%, satellite ranges remain a consistent and attractive destination for Wangiri revenue share termination ranges. Unlike traditional geographic destinations, satellite networks introduce a different kind of challenge — one that is less about location and more about routing and pricing complexity.

Wangiri, by design, relies on the simplicity of a missed call, followed by a callback to a revenue share number. At scale, even a small percentage of successful callbacks can generate significant revenue, but for that model to work, fraudsters require destinations that maximise return. Satellite networks fit that profile perfectly.

Calls to satellite numbers are often associated with significantly higher termination costs compared to standard international routes. What makes satellite networks particularly effective in this model is that they sit slightly outside the typical “known revenue share destination” mindset. While certain country codes may already be flagged or monitored closely, satellite ranges can be less intuitive, less familiar, and therefore less likely to be blocked or scrutinised at the same level by older Fraud Management Systems. At the same time, satellite numbers offer consistently high revenue potential. The result is a reliable fraud vector that does not require constant reinvention.

Much like other forms of IRSF, Wangiri campaigns targeting satellite networks are not necessarily becoming more sophisticated; they are becoming more efficient. As long as call back behaviour remains predictable and high-cost routes remain accessible, the model continues to work.

From a detection perspective, this creates a different kind of challenge: Wangiri traffic can appear low in volume but high in impact. It is distributed, often short-lived, and dependent on user behaviour rather than purely network-generated patterns. When combined with less obvious routing destinations like satellite networks, traditional fraud management systems can struggle to identify risk early enough.

What’s required is a more dynamic understanding of behaviour — identifying suspicious calling patterns, call metric ratios, and anomalous destination profiles in real time.

This is why AB Handshake delivers fully fledged AI-driven fraud detection within its voice product, enabling operators to identify Wangiri campaigns early, including those leveraging satellite networks, before they translate into revenue loss.

SPAM

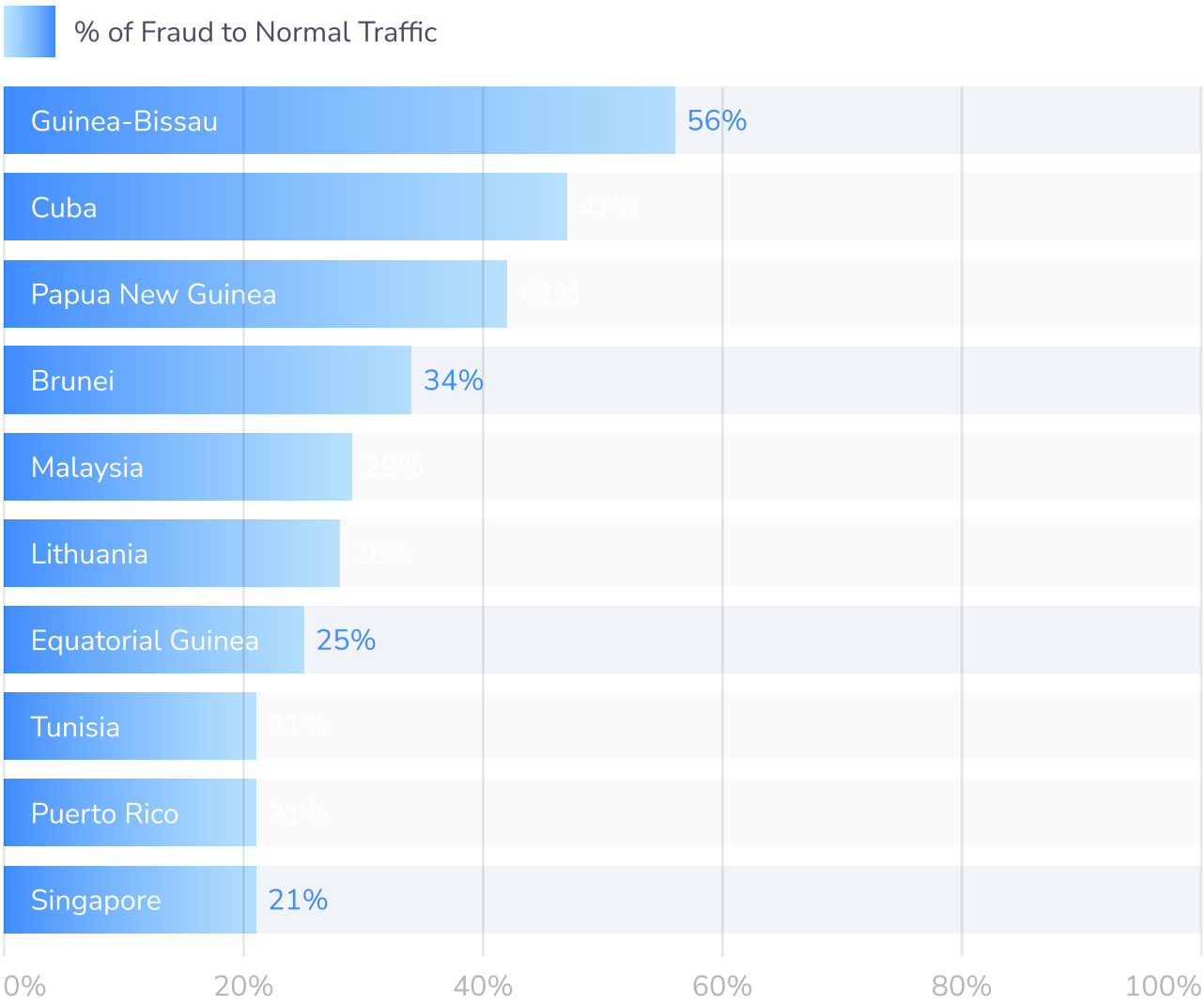
UNDERSTANDING SPAM

Spam traffic typically includes unsolicited robocalls or auto-dialled messages, often used for advertising, scamming, or phishing.

Q1 2026 HIGHLIGHTS

Top receivers for inbound spam: Guinea-Bissau leads with 56%, followed by Cuba at 47% and Papua New Guinea at 42%.

TOP FRAUD DESTINATIONS - % FRAUD TRAFFIC



SPAM TERMINATION IN Q1 2026: RISING SPAM VOLUMES

The Q1 2026 spam termination data points to a clear trend: spam activity continues to increase, both in scale and in how persistently it targets specific routes. While large markets are often associated with high volumes of spam, this dataset highlights a different perspective focused on destinations where spam is particularly concentrated within the traffic mix. Countries such as Guinea-Bissau, Cuba, and Papua New Guinea are not just seeing elevated activity; spam forms a significant part of overall traffic terminating to these routes.

Spam campaigns are deliberately structured to maximise return. Rather than spreading traffic broadly, they focus on destinations where success rates are consistently higher. These tend to be environments where economic incentives are favourable and controls may be less stringent, allowing campaigns to operate with less resistance. Large volumes of traffic are repeatedly directed toward the same destinations, indicating that campaigns are not exploratory; they are structured, predictable, and optimised.

This creates a reinforcing cycle: the more effective a route is, the more traffic it attracts. Over time, certain destinations become heavily associated with spam activity, not necessarily because they carry the most traffic overall, but because they continue to offer reliable outcomes for attackers. From a detection perspective, this presents a timing challenge.

Spam campaigns can be executed quickly, generating high volumes of traffic in short windows. By the time patterns are identified through traditional controls, the activity may already have run its course. This is where static approaches begin to fall short. Destination-based rules and threshold monitoring can highlight known risks, but they often struggle to respond quickly enough to disrupt active campaigns. The real signal lies in behaviour — how traffic repeats, how quickly it scales, and how it deviates from expected patterns over time.

AB Handshake addresses this challenge with fully capable AI-driven spam detection across its voice and SMS products, enabling operators to identify and respond to spam activity in real time, even when it is concentrated on familiar and repeatedly targeted routes.

FLASH CALLS

UNDERSTANDING FLASH CALLS

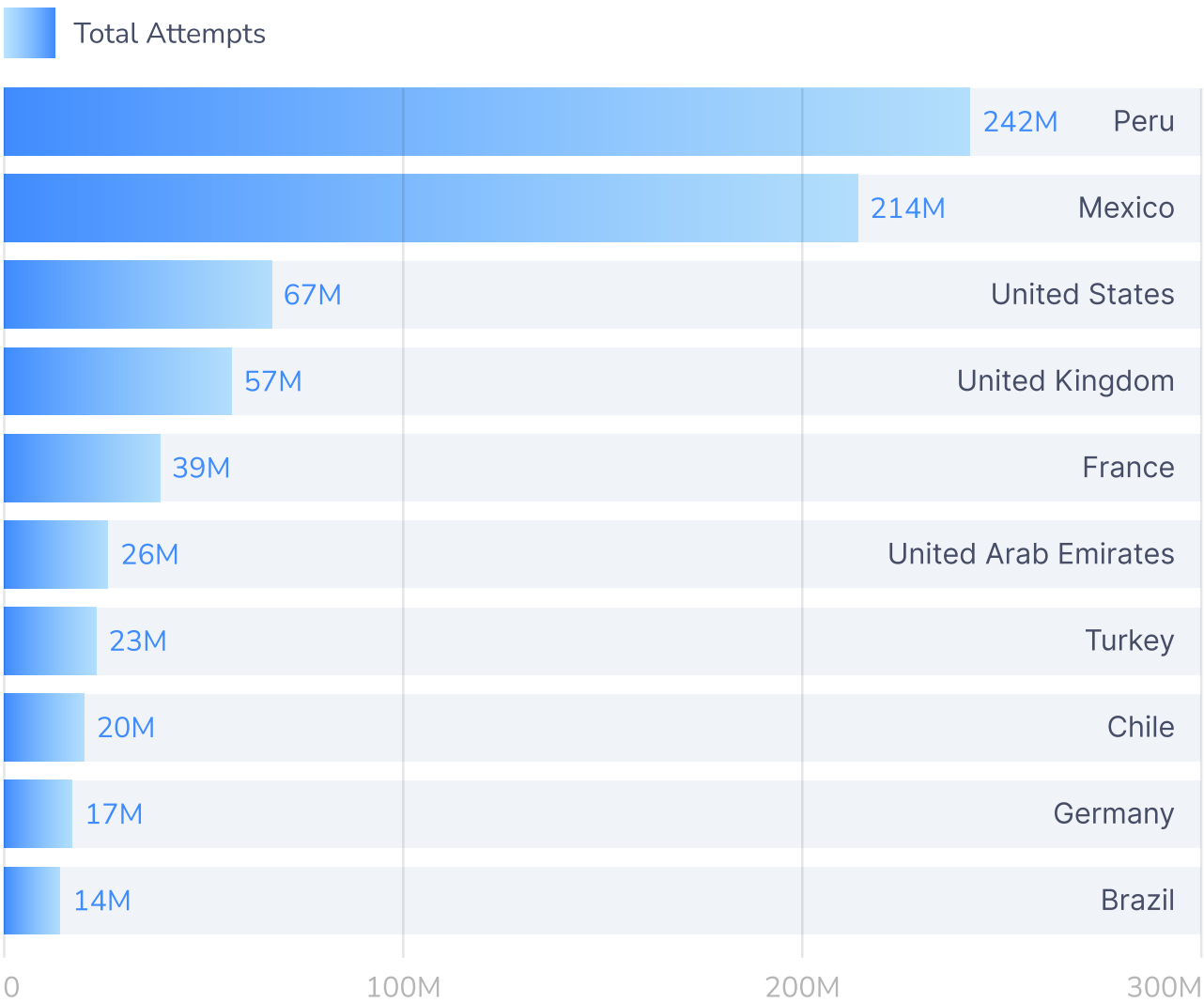
Flash calls are often used for rapid one-time password or two-factor authentication (app sign-ins, one-time password delivery) in place of traditional authentication approaches that rely on A2P SMS delivery.

Q1 2026 HIGHLIGHTS

Top country codes identified as originating this traffic type:
Peru leads with an overwhelming 242M total attempts, followed by Mexico 214M and the United States 67M.

This section ranks the top 10 country range codes where flash call traffic originated, based on total call attempts during the quarter.

TOP ORIGINATING COUNTRIES BY VOLUME



FLASH CALLS

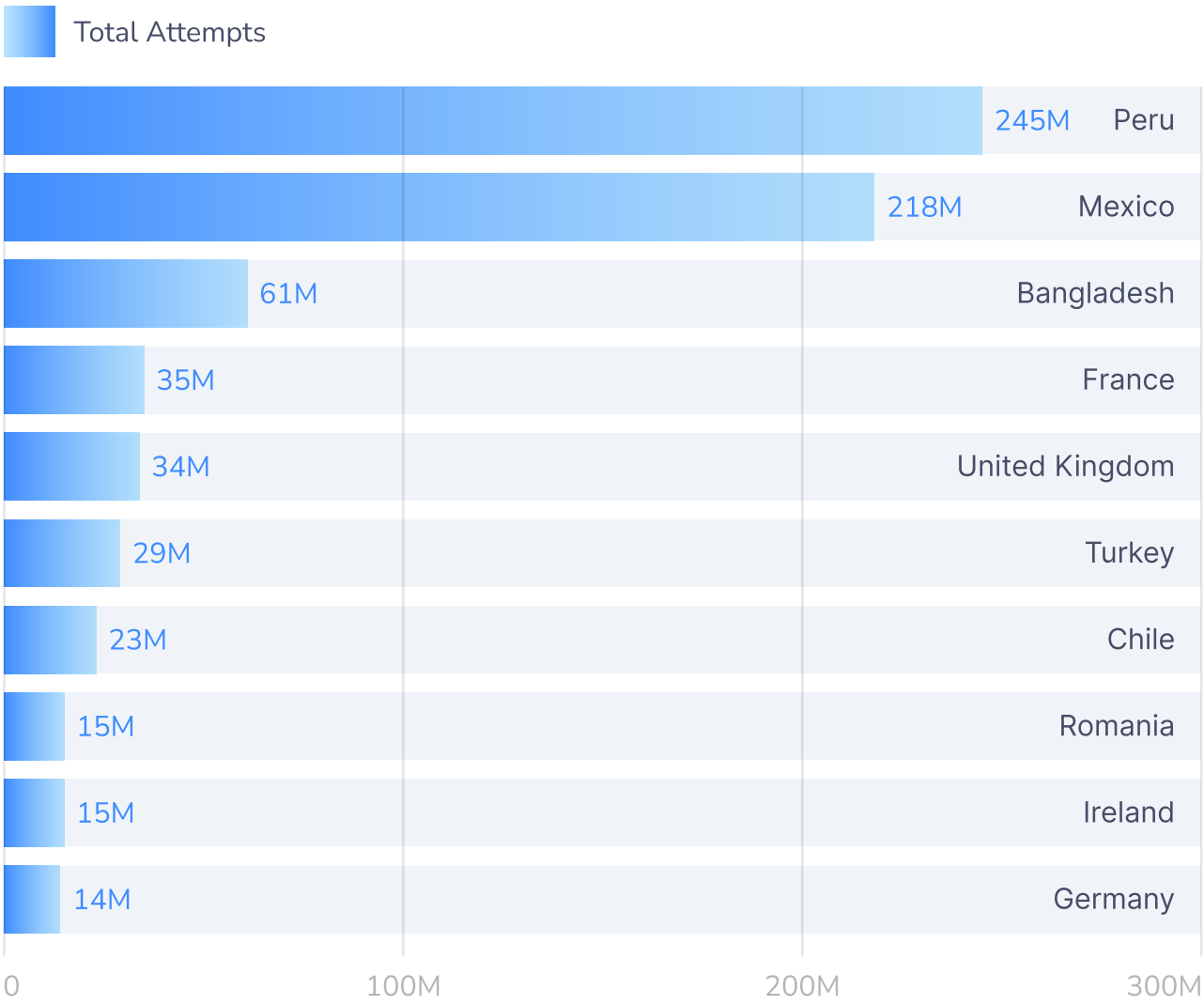
TOP 10 TERMINATION COUNTRIES BY VOLUME OF CALL ATTEMPTS

This section ranks the top 10 countries that received the highest volume of flash call attempts during the quarter.

Q1 2026 HIGHLIGHTS

Peru leads with an overwhelming 245M Total attempts, followed by Mexico at 218M and Bangladesh at 61M.

TOP TERMINATION COUNTRIES BY VOLUME



FLASH CALLS

FLASH CALLING IN Q1 2026: WHY TRADITIONAL VOICE METRICS NO LONGER WORK

Flash calling continues to scale rapidly in Q1 2026, with hundreds of millions of call attempts seen concentrated across a number of markets. Countries like Peru and Mexico dominate both origination and termination volumes, highlighting just how normalised this traffic has become. However, with normalisation comes a problem: the way we traditionally measure and monitor voice traffic simply cannot be applied here.

Conventional telecom metrics such as Answer-Seizure Ratio (ASR), Average Call Duration (ACD), Post-Dial Delay (PDD), and call completion rates are all built around a basic assumption: that a call is intended to be answered and sustained. Flash calls break that assumption entirely, as they are often disconnected before they are answered and are driven by a user request rather than conversation. Their purpose is verification, not communication.

As a result, what would normally be considered “bad” quality metrics in the traffic such as near-zero ASR, near-zero durations, high failure or drop rates — are, in the context of flash calling, completely expected. This is where traditional detection starts to struggle with the challenge of scale complexity. When hundreds of millions of near-identical call attempts are generated, the behaviour itself starts to resemble a stable baseline rather than an anomaly. What once would have stood out now appears normal, and when “normal” includes extremely short, repeated, high-frequency call attempts, distinguishing legitimate use from abuse becomes significantly harder.

Flash calls cannot be managed using static metrics alone, which many traditional detection systems rely on. Flash call handling instead requires an understanding of call patterns over time: velocity, repetition, distribution, and how traffic behaves relative to expected norms across networks and regions.

To address this, AB Handshake provides AI-driven detection within its voice product, allowing operators to identify abnormal behaviour in calling environments, even when traditional metrics fail.

SMS AIT

UNDERSTANDING SMS AIT

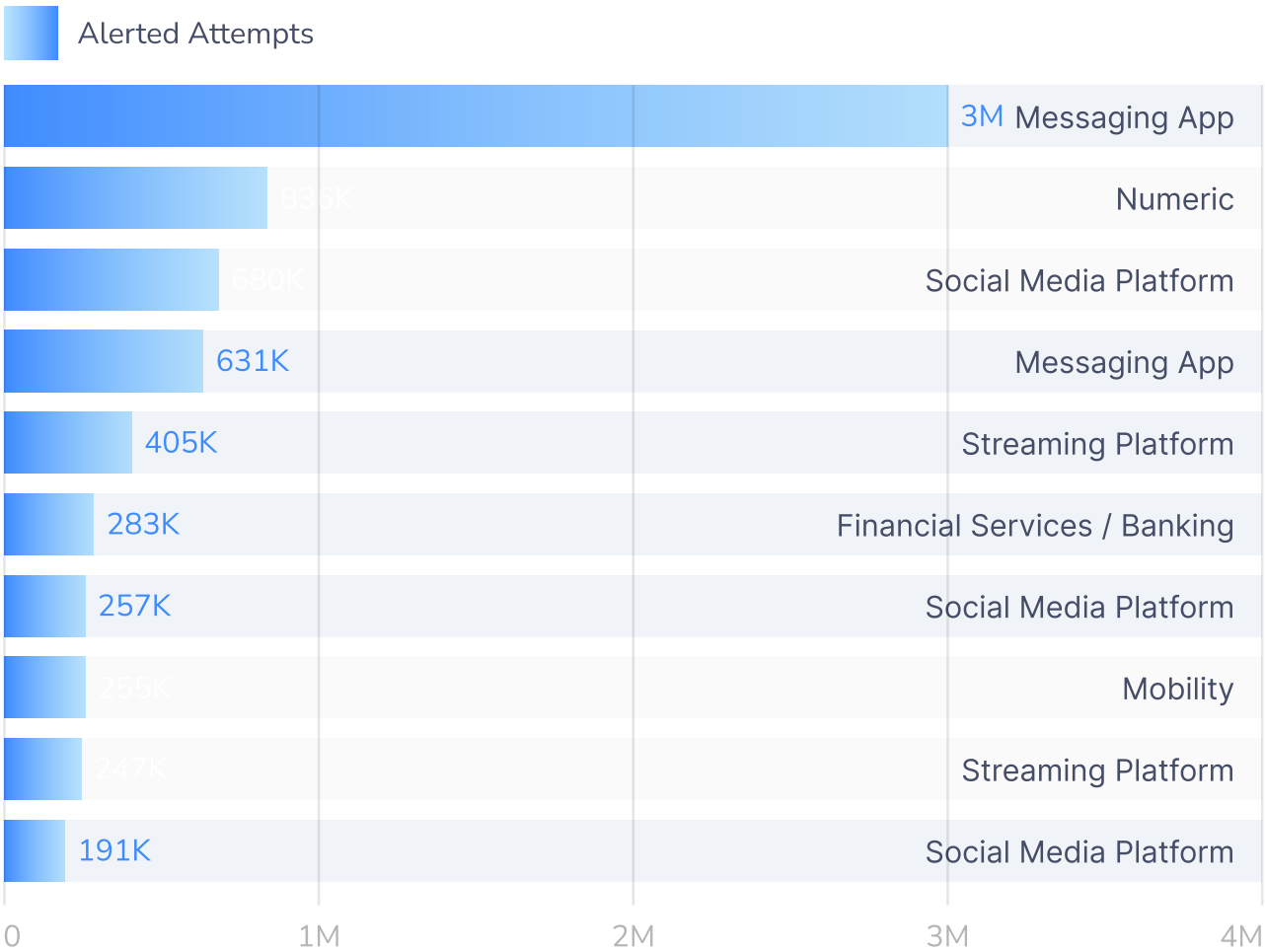
SMS AIT (Artificial Inflation of Traffic) is one of the most structurally damaging fraud types in the telecom ecosystem. Unlike spam or phishing, its goal is not to deceive an end user, but to silently manufacture large volumes by generating large quantities of SMS traffic with no legitimate recipient and no genuine business purpose. SMS AIT occurs as inflated or higher than normal termination volumes, often with no legitimate user behind the traffic.

Q1 2026 HIGHLIGHTS

Top industry senders identified: A Messaging App leads with 3M alerted attempts, followed by Numeric senders at 836K, and Social Media Platform at 680K.

This section lists the top industries most frequently targeted by SMS Artificial Inflation of Traffic (AIT) fraud attempts during the quarter.

TOP SMS AIT FRAUD TARGET BRANDS (ALERTED)



SMS AIT IN Q1 2026: WHEN FRAUD TARGETS TRUST AT SCALE

The latest Q1 2026 data on SMS AIT highlights a clear and growing trend: fraud is no longer just targeting networks, it's targeting brands.

Platforms such as Telegram, Facebook, WhatsApp, and others are seeing significant volumes of artificially generated SMS requests, with millions of alerting attempts recorded in a single quarter. These are not genuine user interactions, but instead automated, systematic attempts to trigger SMS delivery at scale. Targeted brands are commonly globally recognised platforms with massive user bases and frequent authentication flows. Messaging apps, social platforms, and digital services rely heavily on SMS for verification, which makes them ideal entry points for AIT exploitation.

From a fraudster's perspective, this is a highly efficient model. By automating requests, attackers can generate large volumes of SMS traffic without needing to compromise devices or accounts, and each triggered message represents a loss to the service provider.

The fact that a small number of high-profile brands account for a disproportionate share of AIT activity suggests fraudsters are not spreading efforts widely, but are instead focusing on platforms that offer the highest return, the most predictable flows, and the least resistance. Much like other forms of telecom fraud, AIT is not about innovation, it's about optimisation. Because these interactions originate as seemingly legitimate user requests, they are inherently difficult to distinguish from real traffic.

This creates a significant detection challenge for older FMSs. Traditional controls, such as limits, static rules, or basic filtering, can help reduce noise, but they often struggle to keep pace with automated, distributed attack patterns. By the time thresholds are exceeded, substantial volumes of traffic may already have been generated.

For this reason, AB Handshake provides comprehensive, AI-powered fraud detection that enable operators and service providers to identify and respond to AIT campaigns in real time, even when the activity closely mimics legitimate user traffic.

DISCUSSION TOPIC: LANDSCAPE — WHEN "NORMAL" STOPS MEANING SAFE

Looking back at Q1 2026, a clear theme emerges across IRSF, P2S, Wangiri, flash calling, spam, and SMS AIT. While the mechanisms differ, the underlying pattern is strikingly consistent. Fraud is no longer hiding. In fact, in many cases, it is operating in plain sight.

Across datasets, we continue to see traffic routed toward well-known, repeatedly exploited country range destinations, while also leveraging but higher-cost routes such as satellite networks. Spam traffic shows persistent concentration toward specific destinations where it continues to succeed, and in SMS AIT, attackers are not diversifying targets widely, but are instead repeatedly exploiting the same high-volume platforms and brand ecosystems.

Fraudsters are not optimising for stealth, they are optimising for return. Across all these fraud types, one common factor stands out: repetition. High-frequency routes with the same behaviours are being used again and again, suggesting that, from an attacker's perspective, there is little incentive to evolve tactics when existing methods continue to generate revenue. That leads to a more important observation: the challenge is no longer just identifying unknown threats, but is now instead dealing with known ones that continue to work.

Flash call activity highlights this particularly well. At hundreds of millions of attempts, traffic patterns between certain countries have become so large and so consistent that they begin to resemble normal network behaviour. Similarly, SMS AIT traffic originates from legitimate user flows, making it difficult to distinguish between real demand and automated abuse. In P2S, OTP calls appear valid, and across spam attacks and Wangiri, user interaction behaviour completes the loop. In each case, the traffic does not necessarily look suspicious in isolation, but instead looks expected, which is exactly where traditional FMS detection approaches begin to break down.

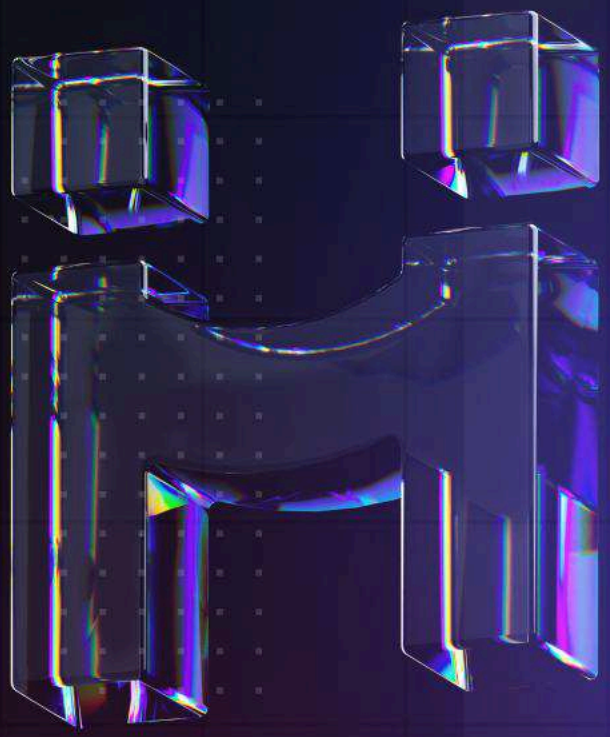
Static rules, country-range destination-based controls, and threshold monitoring all rely on the assumption that fraud will trigger a threshold being breached or a volumetric alert being triggered. When this does not happen as expected, these same fraud management systems may not even be aware that fraud has been missed. This is particularly important as fraud continues to scale through automation.

Across all observed fraud types this quarter, there is a clear move toward low-effort, repeatable attack models. Whether it is bots triggering SMS requests, automated OTP abuse, or mass calling campaigns, the emphasis is on speed and scale rather than complexity. Fraud no longer needs to persist for long periods to be profitable. Short, high-intensity bursts can generate value quickly, often before traditional systems have time to react.

The implication is clear: detection must become faster, more adaptive, and more context-aware.

This is why AB Handshake focuses on AI-driven fraud detection within its voice product, enabling real-time analysis of traffic behaviour across multiple fraud types. By continuously learning patterns and identifying subtle deviations, AI allows operators to detect fraud even when it appears consistent with expected traffic.

AB HANDSHAKE



WANT TO GET EVEN MORE DATA?

Subscribe for weekly reports to see the full picture, including A and B number ranges for all attacks.

Or, sign-up for real-time alerts and block the fraudulent destinations for the duration of the attack. **Don't be a victim of voice fraud!**

CONTACT US

ADDRESS
66 West Flagler Street, Suite 900 — #2329, Miami, FL, USA, 33130

EMAIL
contact@abhandshake.com

ABHANDSHAKE.COM