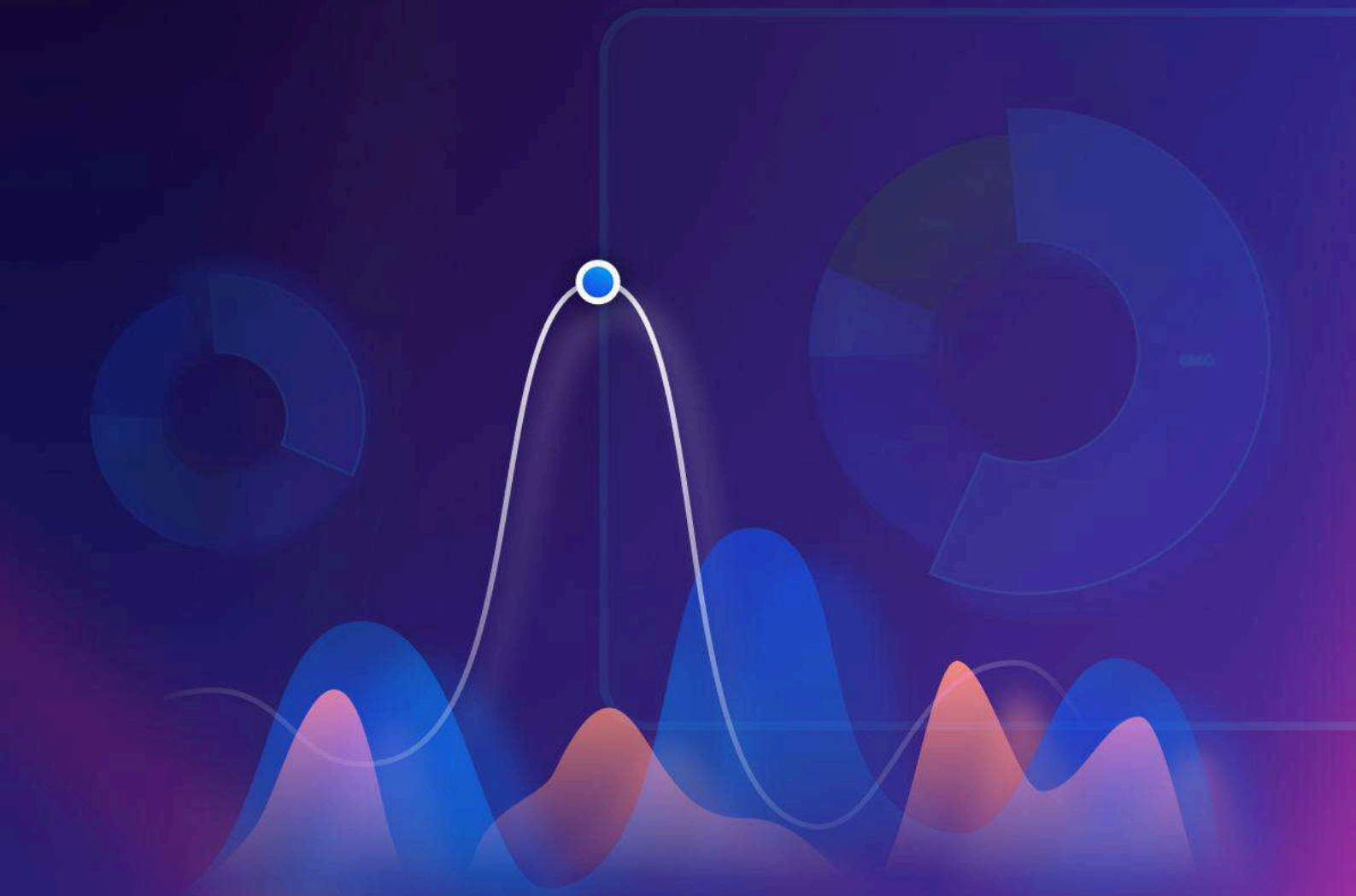
AB HANDSHAKE



FRAUD REPORT Q1 2025

ABHANDSHAKE.COM

Q1 2025 FRAUD REPORT BY AB HANDSHAKE

This read 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 2025 is full of surprising events across our customer base, as we see fraudulent attacks continuing to attempt to break through defenses.

Our Q1 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

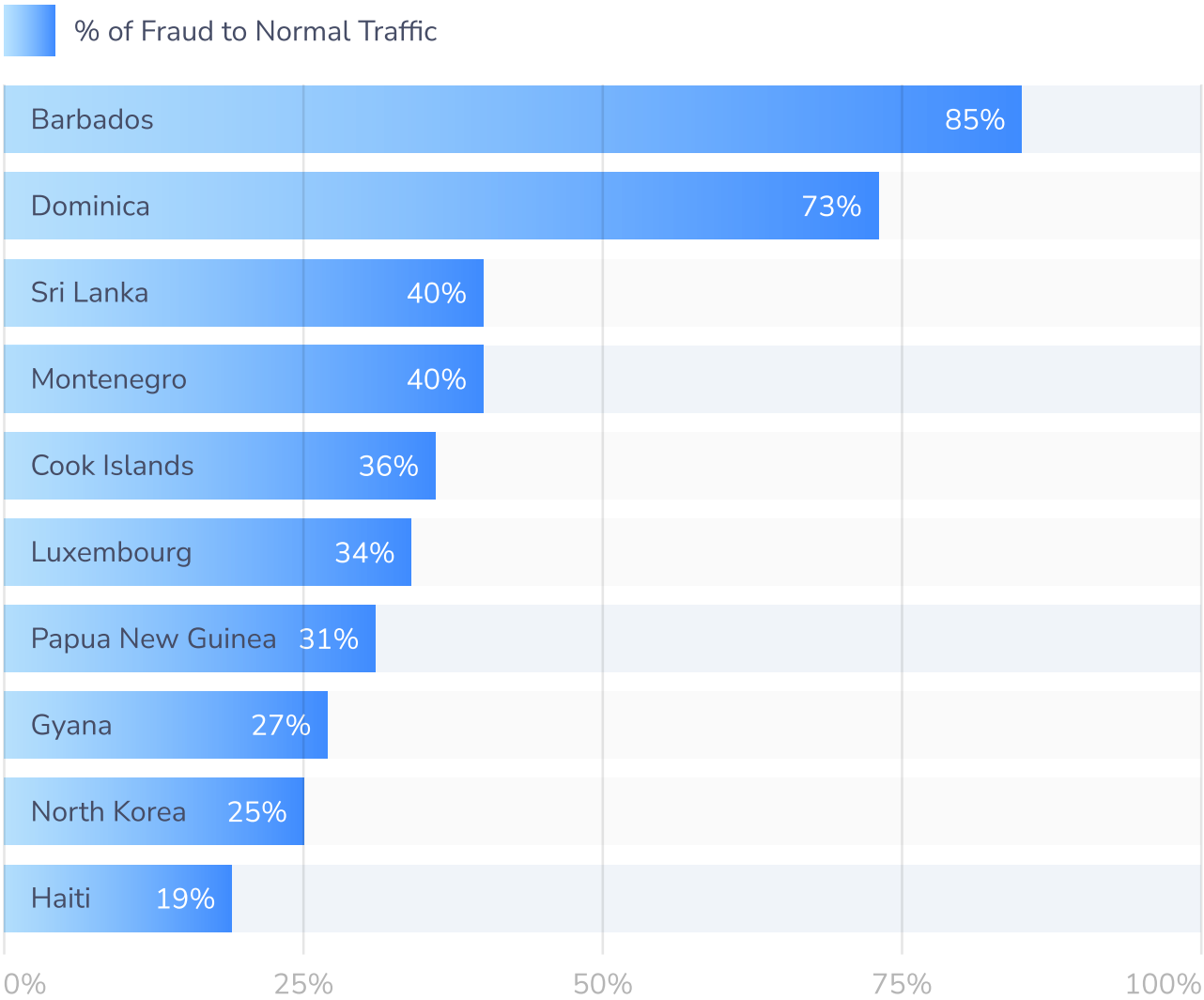
IRSF (International Revenue Share Fraud) typically includes fraudsters artificially driving traffic towards revenue share numbers, which fraudsters gain a profit from. IRSF may also often occur in combination with other fraud types such as Subscription Fraud, Stolen Phones, Roaming events, or PBX Hacking.

Q1 2025 HIGHLIGHTS

Top country codes identified with this traffic type: Barbados led with a fraud ratio of 85%, followed by Dominica at 73% and Sri Lanka at 40%.

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

COMMENTARY

Country ranges with higher interconnect rates are often found on high risk and hot destination lists for just that reason, so those destination ranges will be highly attractive targets for fraudsters conducting International Revenue Share Fraud (IRSF).
As illustrated in the graph, several known high-risk destinations continue to appear prominently, confirming traditional IRSF targeting patterns remain active.

However, a key observation is that the overall proportion of attempted fraudulent IRSF-related traffic terminating to these destination ranges remains low as a percentage of total traffic that is actually connected. This reduction is a direct result of AI-driven detection capabilities within modern Fraud Management Systems (FMS). Prior to the introduction of AI-based detection, IRSF attacks could persist for extended periods, or often several hours or even days. Fraudsters were able to carefully operate below predefined rule-based thresholds (e.g., limiting call attempts per hour) to avoid triggering alerts. By deliberately staying under static monitoring limits, fraudsters could generate substantial fraudulent traffic before detection occurred.

AI-enhanced fraud detection has fundamentally changed this dynamic. Machine learning models identify anomalous traffic patterns in near real time, regardless of whether the activity remains below traditional rule thresholds. This makes the previous evasion approaches largely ineffective. Fraud activity has not stopped, it has just evolved. While fraudsters continue to target obvious high-yield destinations due to their attractive interconnect rates, they are increasingly forced to diversify and disguise their attack patterns.

The key takeaway is that although IRSF attacks persist, AI-driven detection ensures they are identified and contained rapidly. As a result, fraudulent traffic now represents only a very small percentage of overall operator traffic and significantly reduces potential revenue loss exposure.

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, which fraudsters gain a profit from. IRSF may also often occur in combination with other fraud types such as Subscription Fraud, Stolen Phones, Roaming events, or PBX Hacking

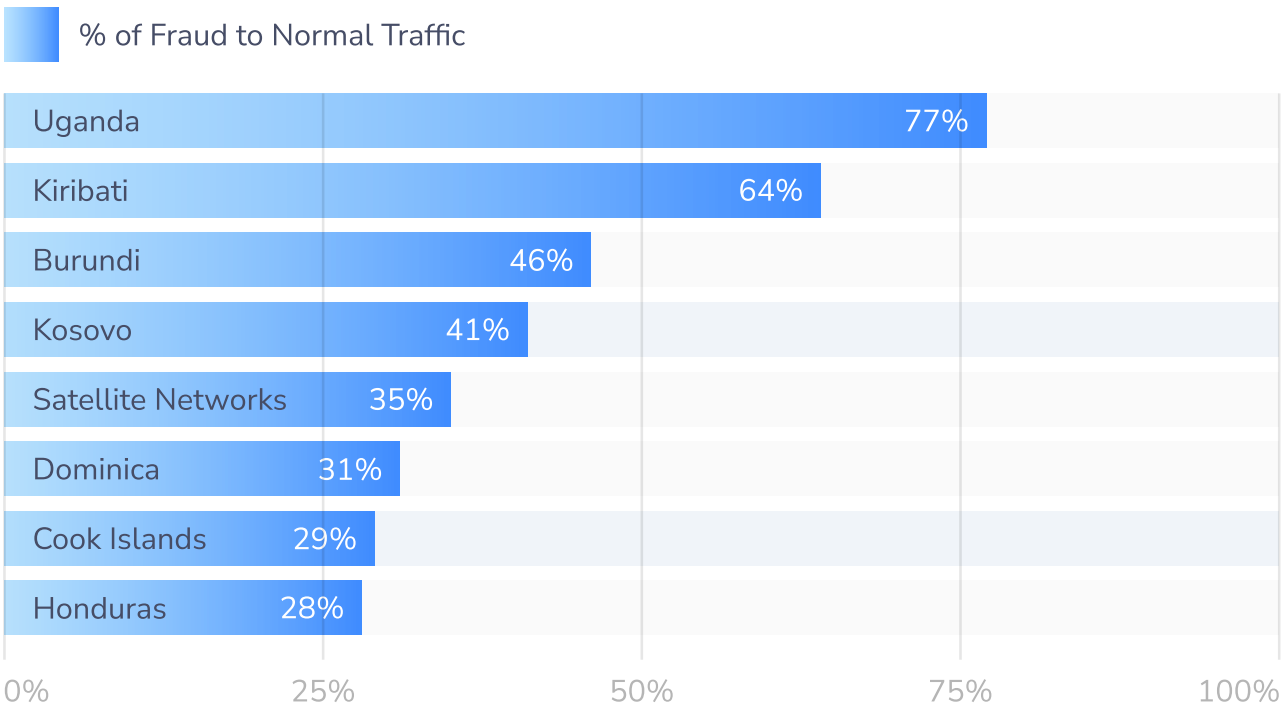
PBX's are often used as a 'fraud method' to commit IRSF, by fraudsters who are able to access badly secured PBX devices inside businesses, and use those to generate artificial traffic towards revenue share numbers. PBX hacking can be identified within typical IRSF attacks as the calls are often timed 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 don't notice constant busy lines during their work day).

Q1 2025 HIGHLIGHTS

Top country codes identified with this traffic type: Uganda recorded the highest ratio at 77%, followed by Kiribati at 64% and Burundi at 46%.

The following dashboard identifies the top 8 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

COMMENTARY:

PBX hacking enabled IRSF is typically opportunistic in nature, driven primarily by the discovery of poorly secured or misconfigured PBX systems such as those with PINs of Passwords like 1234 or 0000. Once access is obtained, fraudsters generate artificial traffic toward revenue share destinations, selecting countries based largely on the availability of monetizable number ranges rather than geographic targeting strategy.

During this quarter, PBX hacking enabled IRSF activity continued to impact multiple customers and resulted in traffic terminating across a broad range of global destination ranges. The data indicates that Uganda recorded the highest concentration of PBX-related IRSF activity, with more than 77% of all traffic terminating there as PBX-driven IRSF traffic.

This represents a significant proportion of total traffic to a single destination and highlights the scale of exposure where PBX vulnerabilities exist from where this traffic is originating from. It may also signal elevated risk for operators that do not deploy AI-driven IRSF detection capabilities in those locations. Fraudsters frequently reuse successful attack methodologies across multiple operators, systematically targeting networks in search of weaker detection controls.

AI-infused fraud detection systems such those offered by AB Handshake significantly mitigate this risk by rapidly identifying abnormal traffic signatures associated with PBX compromise, thereby limiting duration, financial exposure, and downstream revenue impact.

P2S

UNDERSTANDING P2S

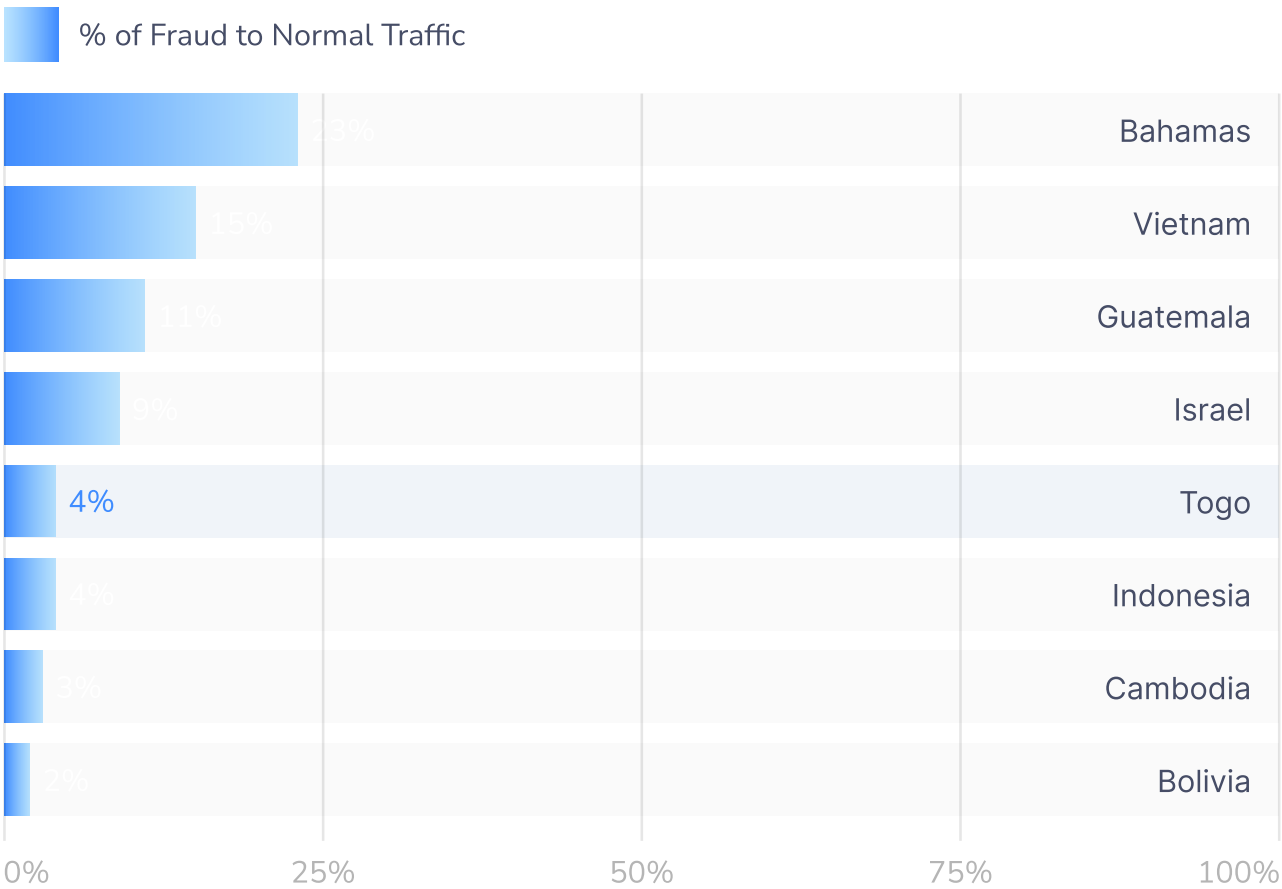
P2S attacks typically involve automated bots or scripts abusing web forms or online verification processes to trigger voice-based OTP calls to revenue share numbers, which the fraudsters will gain revenue from. Such patterns often reveal systematic P2S attacks, where repeated automated attempts focus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

Q1 2025 HIGHLIGHTS

Top country codes identified with this traffic type: Bahamas recorded the highest ratio at 23%, followed by Vietnam at 15% and Guatemala

The following dashboard identifies the country ranges with P2S

TOP FRAUD DESTINATIONS - % FRAUD



P2S

COMMENTARY

Several well-established high-risk revenue share destinations appear within this quarter's list of P2S destination revenue share numbers, and are historically associated with elevated exposure to revenue share fraud.

P2S fraud methods exploit legitimate online systems that provide automated PIN delivery via outbound voice calls. Fraudsters manipulate these platforms such as account verification, password reset, or authentication services by repeatedly submitting revenue share numbers to the P2S system. Those systems then automatically place outbound calls to deliver the PIN via speech to these provided numbers, unintentionally generating calls towards revenue share numbers the fraudster will gain revenue from.

Unlike PBX hacking, P2S fraud does not require network compromise. Instead, it exploits weaknesses in publicly accessible online services, particularly where there is insufficient validation, call limiting, behavioural monitoring, or number screening. As the resulting traffic terminates to revenue share ranges, it is often grouped alongside IRSF and PBX-related fraud in reporting, however the attack method's vector is distinct and requires different mitigation strategies.

This quarter's findings confirm that P2S fraud remains active and opportunistic.
The primary vulnerability lies in inadequate controls around automated outbound calling mechanisms. Organisations that do not prioritise strong input validation, traffic throttling, bot detection, and anomaly monitoring remain highly susceptible.

Once fraudsters identify a vulnerable PIN delivery system, traffic volumes can scale rapidly, leading to significant revenue exposure before traditional controls detect abnormal patterns. This reinforces the importance of AI-driven behavioural analytics and proactive traffic monitoring systems such as AB Handshake's to quickly identify and suppress abnormal P2S activity.

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.

These callbacks are then monetized by keeping the line active, often using ringing tones or recorded loops to extend call duration and entice the caller to ‘stay on the line’.

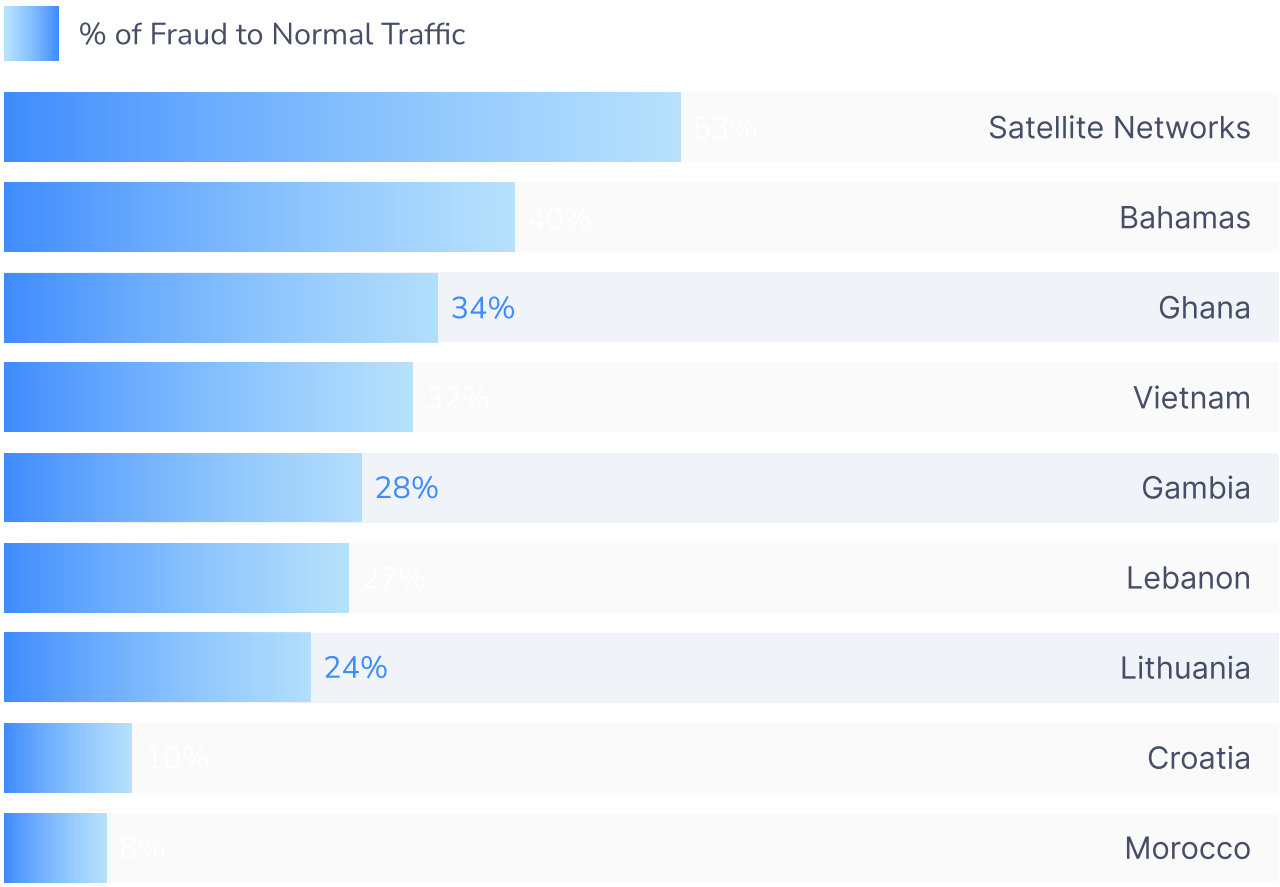
Q1 2025 HIGHLIGHTS

Top country codes identified with this traffic type: Satellite Networks lead with 53%, followed by Bahamas at 40% and Ghana at 34%.

This section displays the top 9 country range codes where Wangiri 2.0 callback fraud made up the largest share of total traffic during the quarter.

WANGIRI 2.0 ACTIVITY

TOP FRAUD DESTINATIONS - % FRAUD



WANGIRI 2.0

COMMENTARY

Wangiri 2.0 activity continues to be observed across multiple customers this quarter. Unlike traditional missed-call Wangiri fraud, this variation exploits online number input forms and automated callback systems to trigger outbound calls to revenue share numbers purchased by fraudsters.

Several destination ranges identified in this quarter's findings are well-established high-risk ranges for revenue share fraud. The recurrence of these destinations reinforces the pattern that fraudsters consistently target jurisdictions with attractive interconnect rates and accessible revenue share number ranges.

Notably, the same high-risk destinations detected under Wangiri 2.0 could equally be used in other IRSF methodologies, such as PBX hacking or P2S to name a few. The underlying monetisation model remains consistent however of artificially inflating traffic to revenue share numbers.

This demonstrates that IRSF is method-agnostic. As long as exploitable entry points exist. Whether network-level, enterprise-level, or end-user-level, fraudsters will continue to repurpose established high-risk destinations across multiple fraud techniques. Continuous monitoring, AI-driven anomaly detection, and layered preventative controls remain critical to limiting exposure and containing revenue loss like AB Handshake's Fraud Managements system.

SPAM

UNDERSTANDING SPAM

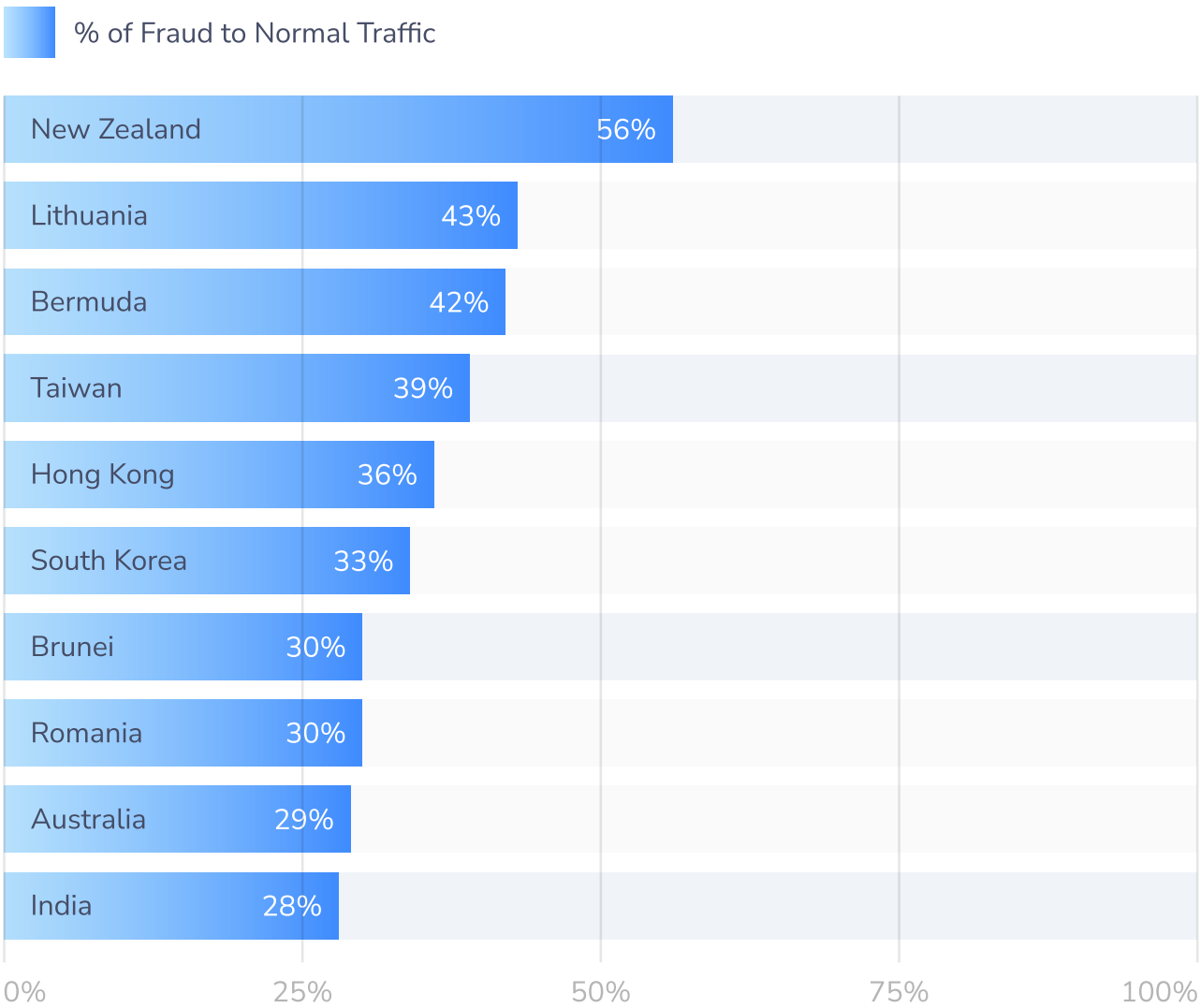
Spam traffic typically includes unsolicited robocalls or auto-dialed messages, often used for advertising, scamming, or phishing.

Q1 2025 HIGHLIGHTS

Top country codes identified with this traffic type: New Zealand leads with 56%, followed by Lithuania at 43% and Bermuda at 42%.

This section shows the top 10 country range codes where spam calls accounted for the highest percentage of total inbound traffic during the quarter.

TOP FRAUD DESTINATIONS - % FRAUD



SPAM

COMMENTARY

New Zealand, Lithuania and Bermuda lead this quarter's list of spam-terminating destinations. This is not unexpected, as these markets amongst many others have long experienced elevated levels of spam and scam-related traffic.

From a fraudster's perspective, the dominance of these three destinations reveals diverse targets, with likely a higher return identified for investments. When highly divergent locations are targeted such as these at such high levels, it many indicate the reuse of similar large scale attacks which could also reduce operational complexity and increases scalability from the fraudster's perspective. The data from this quarter reinforces the concept of "reuse," where successful scam methodologies are repeatedly deployed across similar markets to maximise return on investment.

By detecting pattern reuse across multiple country ranges, AI-driven systems significantly improve early identification and suppression of scam traffic. While spam activity remains persistent in these high-volume markets, advanced behavioural analytics offered by fraud management systems like AB Handshake's continue to strengthen prevention and reduce the overall impact of fraud.

FLASH CALLS

UNDERSTANDING FLASH CALLS

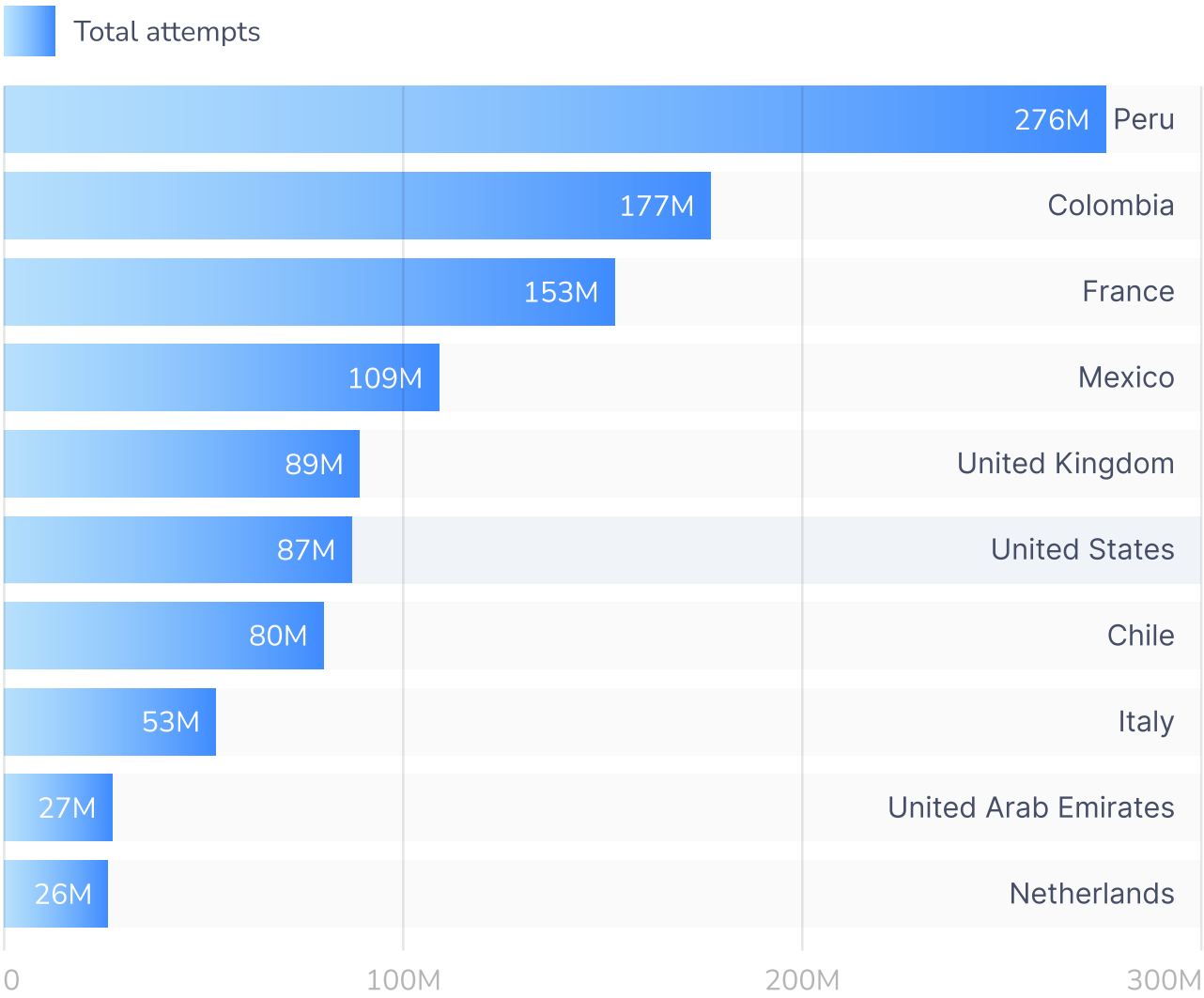
Flash calls are often used for rapid one time password or two factor authentication (app sign-ins, one time password delivery) in place of traditional authentication approaches which rely on A2P SMS delivery.

Q1 2025 HIGHLIGHTS

Top country codes identified with originating this traffic type: Peru leads with an overwhelming 278M Total attempts, followed by Colombia 177 M and France 153M.

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

COMMENTARY

Flash Calls continue to grow quarter over quarter, with both overall generation volumes and detection rates increasing consistently. This sustained growth highlights their expanding role within the authentication and messaging ecosystem.

In the latest quarter, flash call volumes were particularly significant from specific country codes. More than 276 million flash calls were generated from Peru country codes alone, followed by over 177 million from Colombia and approximately 153 million from France. These figures demonstrate the scale at which flash call based verification mechanisms are now operating globally.

As flash calls become more embedded in standard authentication workflows, particularly for one-time password (OTP) verification, we are observing recurring source patterns across networks.

How operators respond remains an evolving strategic decision. Outcomes will depend heavily on the detection methodologies deployed and the decisions made by various Operator's on how this traffic continues. Advanced detection capabilities are increasingly essential to maintaining network integrity while supporting legitimate use cases.

SMS AIT

UNDERSTANDING SMS AIT

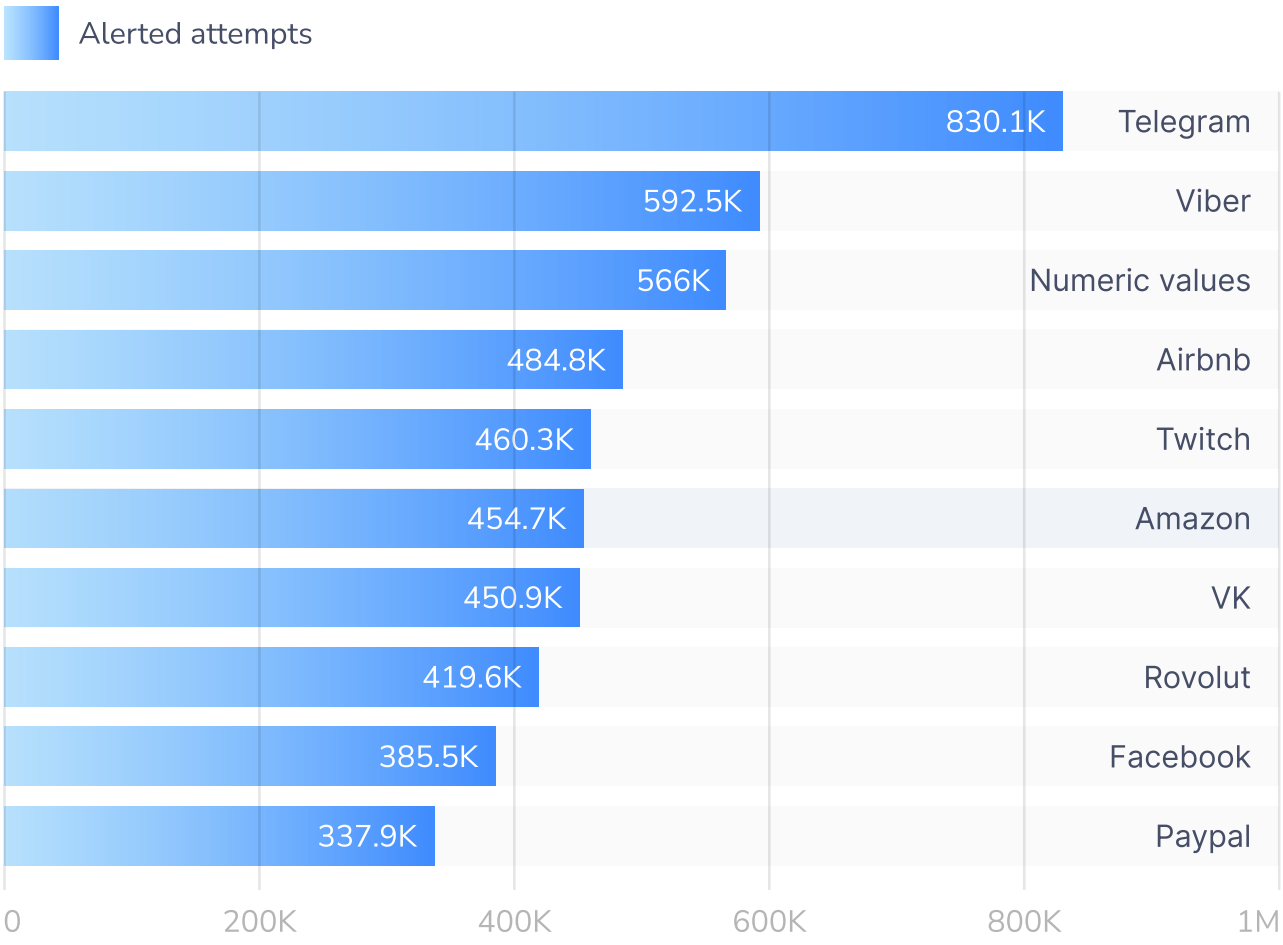
SMS AIT (Artificial Inflation of Traffic) is one of the most structurally damaging fraud types in the telecom ecosystem. Unlike spam or phishing, its goal is not to deceive an end user, but to silently manufacture large volumes by generating large quantities of SMS traffic with no legitimate recipient 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 2025 HIGHLIGHTS

Top senders identified: Telegram leads with 830 K alerted attempts, followed by Viber 592 K and numeric 566 K.

This section lists the top 10 brands most frequently targeted by SMS Artificial Inflation of Traffic (AIT) fraud attempts during the quarter.

TOP TARGETED BRANDS FOR SMS AIT FRAUD



SMS AIT

COMMENTARY

SMS Artificially Inflated Traffic (AIT) continues to present a significant risk to brands and application-to-person (A2P) senders. The financial and reputational impact can be substantial, particularly where high volumes of one-time passwords (OTPs), verification codes, or account sign-up messages are generated artificially.

This exposure affects both large, established platforms such as Telegram and smaller or emerging brands. While major enterprises are frequently targeted due to their scale and predictable authentication flows, smaller organisations are often more vulnerable due to limited awareness of SMS AIT risks and insufficient monitoring controls.

In typical AIT scenarios, fraudsters automate account creation, password reset, or verification workflows to trigger large volumes of SMS traffic. Without appropriate traffic validation or behavioural monitoring, this activity can escalate rapidly, generating substantial artificial traffic and inflated messaging costs.

The key risk factor remains visibility. Organisations that lack real-time monitoring, anomaly detection, and AI-driven behavioural analytics like those of AB Handshake remain unaware that their platforms are being abused. Proactive detection mechanisms are therefore critical, not only to prevent direct financial loss, but also to protect brand reputation and maintain the integrity of authentication systems.

Q1 2025 DISCUSSION TOPIC: THE VALUE OF SHARED FRAUD DETECTION

One of the most significant advantages of deploying an established, AI-driven fraud detection platform is the ability to share intelligence across multiple operators and customers. Fraud is rarely isolated. As demonstrated throughout this quarter's findings across IRSF, PBX hacking, P2S abuse, Wangiri 2.0, and even SMS AIT, fraudsters consistently reuse successful destinations, number ranges, and behavioural patterns.

Well established high-risk destinations for artificially inflated traffic frequently appear on this report, while the entry point varies. Whether the attack vector is a compromised PBX, an exploited PIN-to-Speech platform, a vulnerable online callback form, SMS authentication abuse, or spam campaigns, the underlying patterns of reuse are clear.

This is where shared fraud detection becomes strategically powerful, and leveraging reliable fraud detection and revenue loss prevention systems like those at AB Handshake.

PREVENTING REUSE ACROSS CUSTOMERS

Fraudsters frequently deploy the same attack methodology across multiple operators in quick succession, seeking networks with weaker controls. In isolated detection environments, each operator must independently identify and respond to the threat, often after exposure has already occurred.

In contrast, a shared AI-driven detection ecosystem enables immediate cross-customer protection. Once anomalous behaviour is identified in one network, such as unusual ASR/ALOC patterns, sudden traffic spikes to a high-risk destination, surges from specific country codes, or abnormal patterns, the intelligence can inform protective models across all connected customers.

AI AS A NETWORK EFFECT MULTIPLIER

Advanced AI models do not rely solely on static thresholds. Instead, they detect behavioural anomalies regardless of the specific entry point or methods used to conduct the fraud.

The more networks and traffic profiles the system observes, the stronger and faster the models become. Each detected anomaly improves pattern recognition across the ecosystem. As seen in this quarter's results, although fraud attempts continue, the percentage of fraudulent traffic relative to total traffic remains low which demonstrates rapid identification and suppression.

This network-wide intelligence sharing creates a protective multiplier effect:

- When one customer is targeted, all customers benefit.
- When a new fraud pattern emerges, it is learned once and applied globally.
- When high-risk destinations resurface, models adapt immediately.

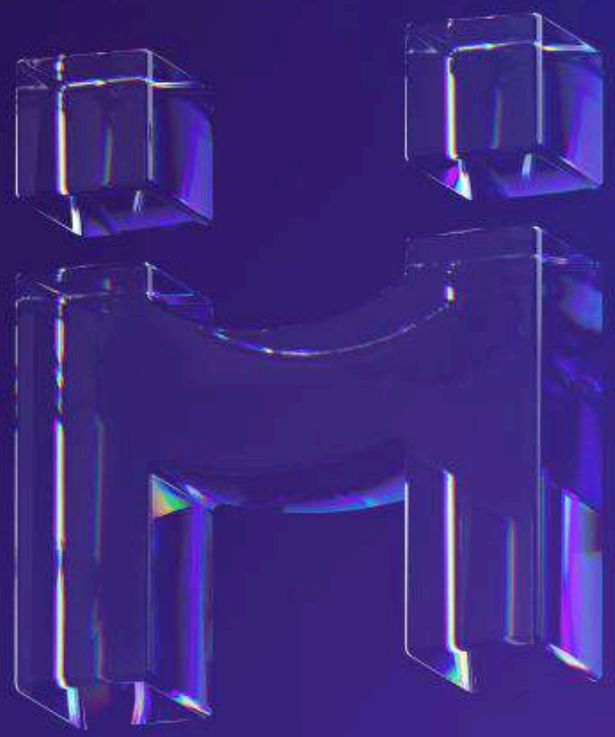
STRATEGIC TAKEAWAY

Fraud will continue to evolve, however the common thread remains reuse and monetisation of known high-yield destinations.

An established, shared AI-driven fraud detection platform transforms this challenge into an advantage. By leveraging cross-network intelligence and behavioural anomaly detection, operators are no longer defending in isolation, they are operating within a collaborative, adaptive defence framework that significantly limits fraud duration, scale, and financial impact.

In a landscape where fraud never stops but continually changes form, shared AI-driven detection ensures that protection evolves faster than the threat.

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