AB HANDSHAKE

FRAUD REPORT

Q3 2025

ABHANDSHAKE.COM

Q3 2025

AB Handshake releases a special Flash Call-focused quarterly report, also featuring the latest findings on emerging fraud trends across Spam and Wangiri attacks.

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 sleeps. What changes is the how. Q3 2025 is full of surprising events across our customer base, as we observe fraudulent attacks continue trying to break through defenses.

Our Q3 2025 review focuses on the major fraud vectors observed in voice and SMS traffic monitored by the 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:

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.

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.

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.

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

Apply

IF YOU WOULD LIKE TO SUBSCRIBE TO OUR WEEKLY REPORTS:

Subscribe

SPAM

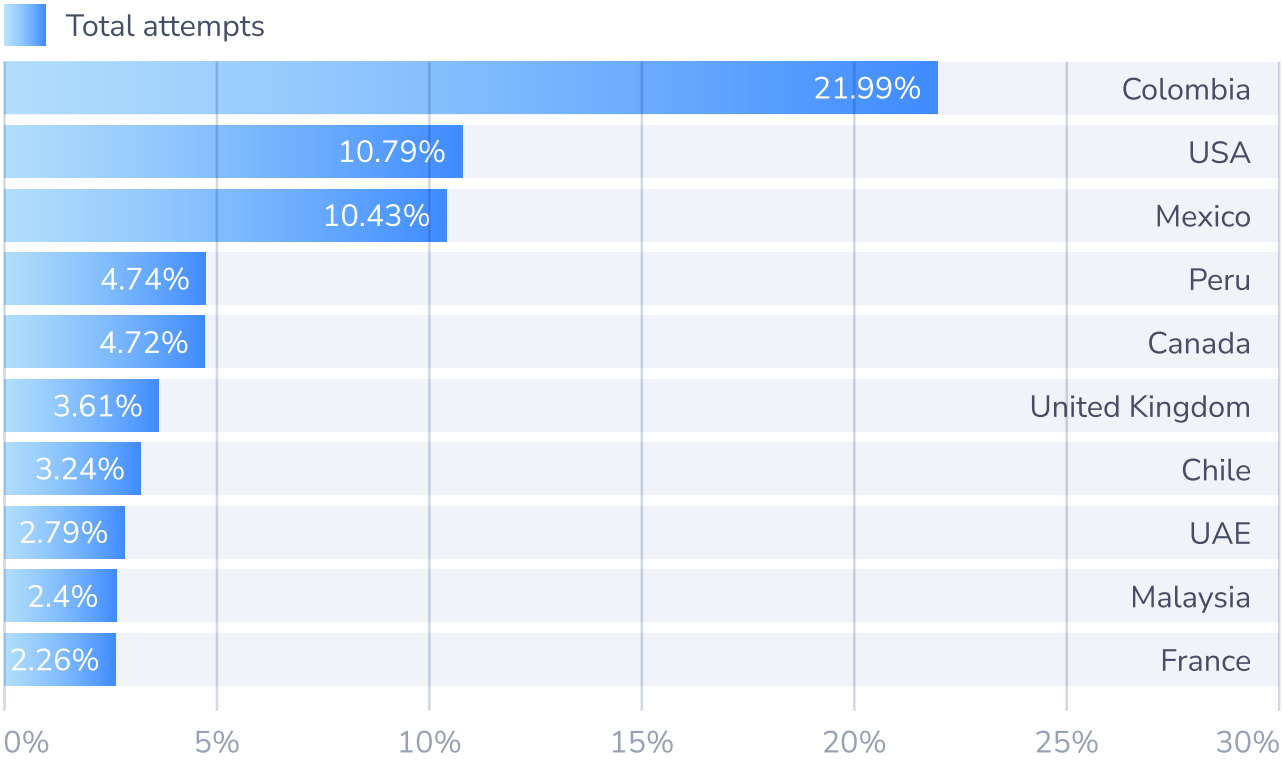
WHAT IT IS

Spam traffic typically includes unsolicited robocalls or autodialed messages, often used for advertising, scamming, or phishing. These calls may not always result in monetary loss, but they disrupt operations and harm user trust.

Q3 HIGHLIGHTS

Top receivers of inbound spam: Colombia led with 21.99%, followed by the USA (10.79%) and Mexico (10.43%).

TOP 10 COUNTRIES RECEIVING INBOUND SPAM, RELATIVE TO ALL SPAM TRAFFIC



WHAT THE DATA TELLS US

The USA has historically been a major target for spam traffic, which in part drove the development of the STIR/SHAKEN framework. However, the Q3 data suggests that spam remains a persistent challenge, indicating that STIR/SHAKEN alone is not sufficient to fully prevent these attacks. Interestingly, Colombia accounts for roughly twice the share of observed inbound spam compared with the average US subscriber, highlighting how spam patterns are shifting geographically. This may suggest that while STIR/SHAKEN has helped reduce the impact of spam in some markets, additional strategies and detection measures are still required to address the evolving threat.

WANGIRI INBOUND ATTACKS

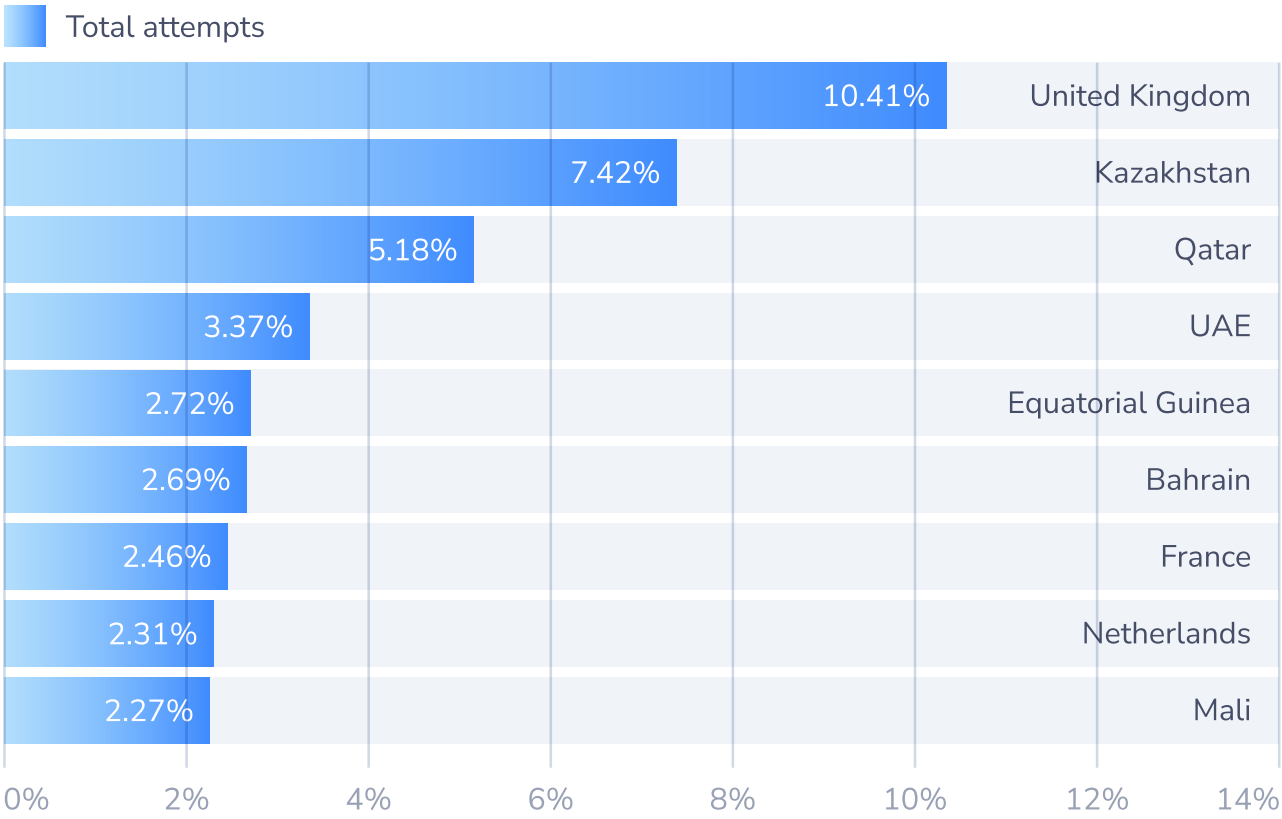
WHAT IT IS

Wangiri fraud works by triggering short one-ring calls or missed calls to users from revenue-share numbers, enticing them to call back. Those who do return these calls do not realize they are calling a revenue-share number from which the fraudster profits.

Q3 HIGHLIGHTS

Top receivers of inbound Wangiri attacks as a percentage of all inbound traffic: The UK leads with 10.41%, followed by Kazakhstan (7.42%).

TOP 10 COUNTRIES RECEIVING INBOUND WANGIRI ATTACKS, RELATIVE TO ALL INBOUND TRAFFIC



WHAT THE DATA TELLS US

Wangiri attempts continue to lure unsuspecting users into calling back revenue-share numbers, generating profit for fraudsters with every returned call. What stands out in the data this quarter is the noticeable absence of certain countries, such as the USA, among the top targets of inbound Wangiri attacks. This may suggest that proactive anti-fraud measures, such as STIR/SHAKEN and ongoing regulatory collaboration, are having a deterrent effect. When countries take visible steps to strengthen their defenses and openly address these scams, it appears that fraudsters may shift their attention elsewhere, avoiding markets that have become too costly or complex to exploit.

FLASH CALLS AND THE COUNTRIES THEY TERMINATE TO — THE SILENT, UNMONETIZED 2FA LOOPHOLE

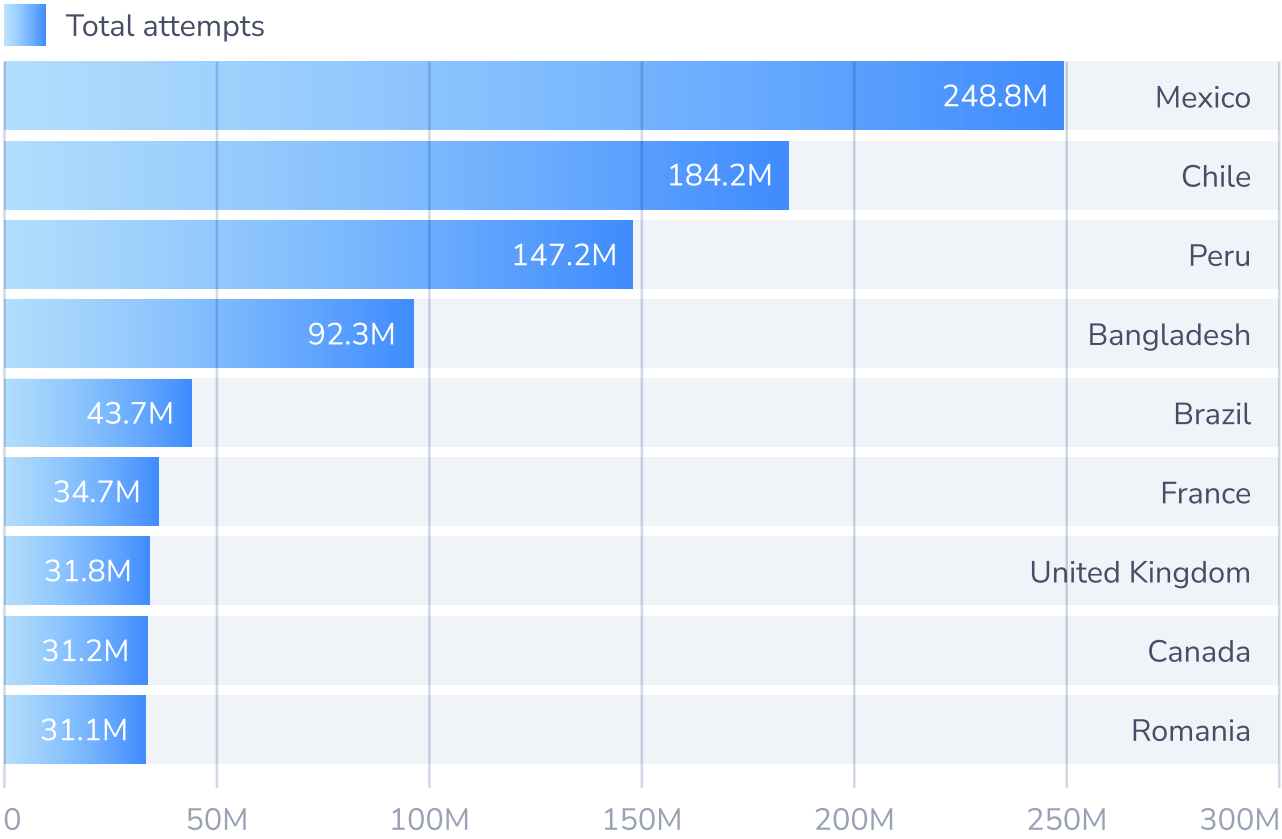
WHAT IT IS

Flash calls are often used legitimately for rapid verification (app sign-ins, one-time password delivery). Fraudsters abuse this mechanism to generate silent calls at scale or to farm responses from carriers and APIs.

Q3 HIGHLIGHTS

Top destinations for Flash Calls: Mexico leads with an overwhelming 248.8M total attempts, followed by Chile (184.2M) and Peru (147.2M).

TOP 10 DESTINATION COUNTRIES BY FLASH CALL VOLUME



WHAT THE DATA TELLS US

Flash Calls continue to surge, with 248.8 million calls terminated to Mexico this quarter alone. Analysis of our customer networks shows that countries in Central and South America are being targeted most heavily, while much of Europe is experiencing comparatively lower volumes. This pattern highlights a regional concentration of Flash Call activity and underscores the need for targeted fraud detection and mitigation strategies in the hardest-hit markets.

FLASH CALLS AND THE COUNTRIES THEY ORIGINATE FROM

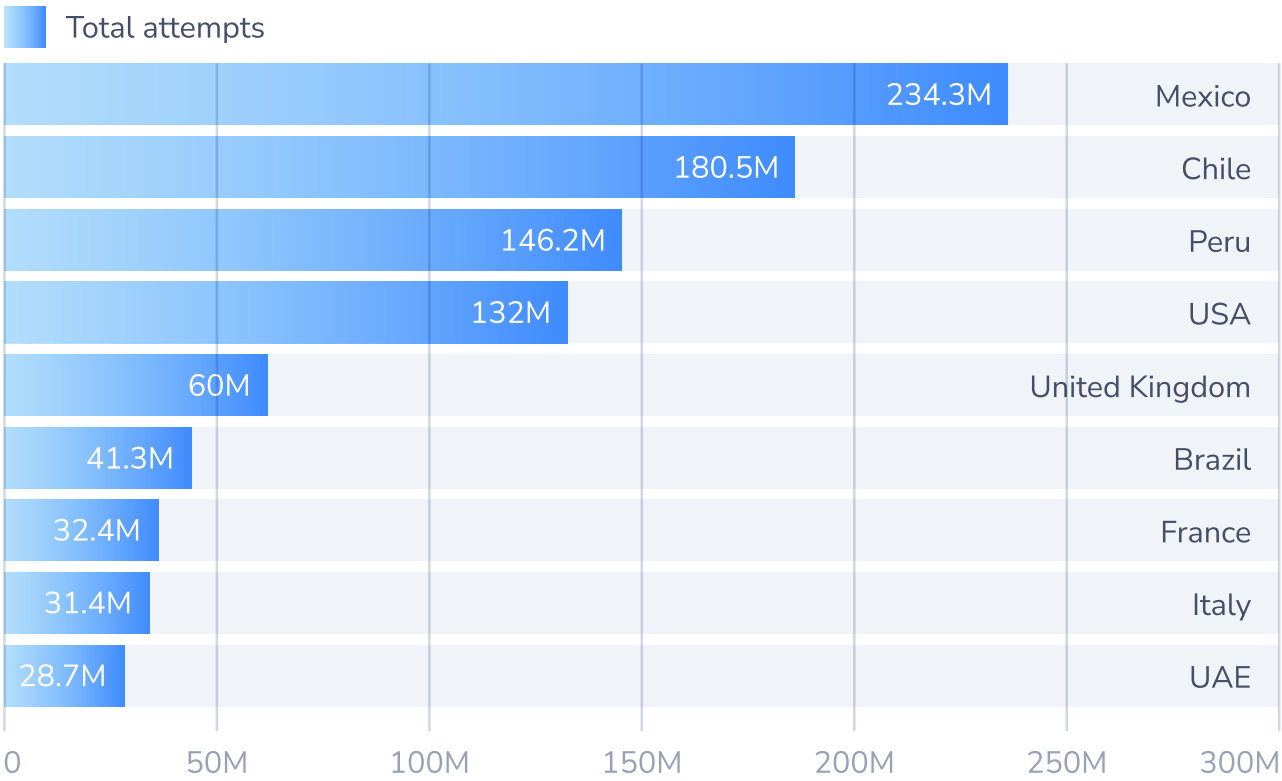
WHAT IT IS

Flash calls are often used legitimately for rapid verification (app sign-ins, one-time password delivery). Fraudsters abuse this mechanism to generate silent calls at scale or to farm responses from carriers and APIs.

Q3 HIGHLIGHTS

Top origins of Flash Calls: Mexico leads with an overwhelming 234.3M total attempts, followed by Chile (180.5M) and Peru (146.2M).

TOP 10 ORIGINATING COUNTRIES BY FLASH CALL ATTEMPTS



WHAT THE DATA TELLS US

Analysis of Flash Call originations highlights a strong overlap between the top sending and receiving countries, namely Mexico, Chile, and Peru. These countries are not only generating massive volumes of Flash Calls but are also among the primary destinations, indicating a potentially self-contained cycle of fraud.

The scale and persistence of this activity underscore the urgent need for effective mitigation. Fraud continues to grow where preventative measures are absent, and the detection of this traffic by AB Handshake demonstrates that many existing fraud systems are currently unable to identify or block these sophisticated operations effectively. Without targeted intervention, fraudsters continue to view these schemes as highly profitable and low-risk.

FLASH CALLS: LOCAL NUMBER ORIGINATION AND TERMINATION

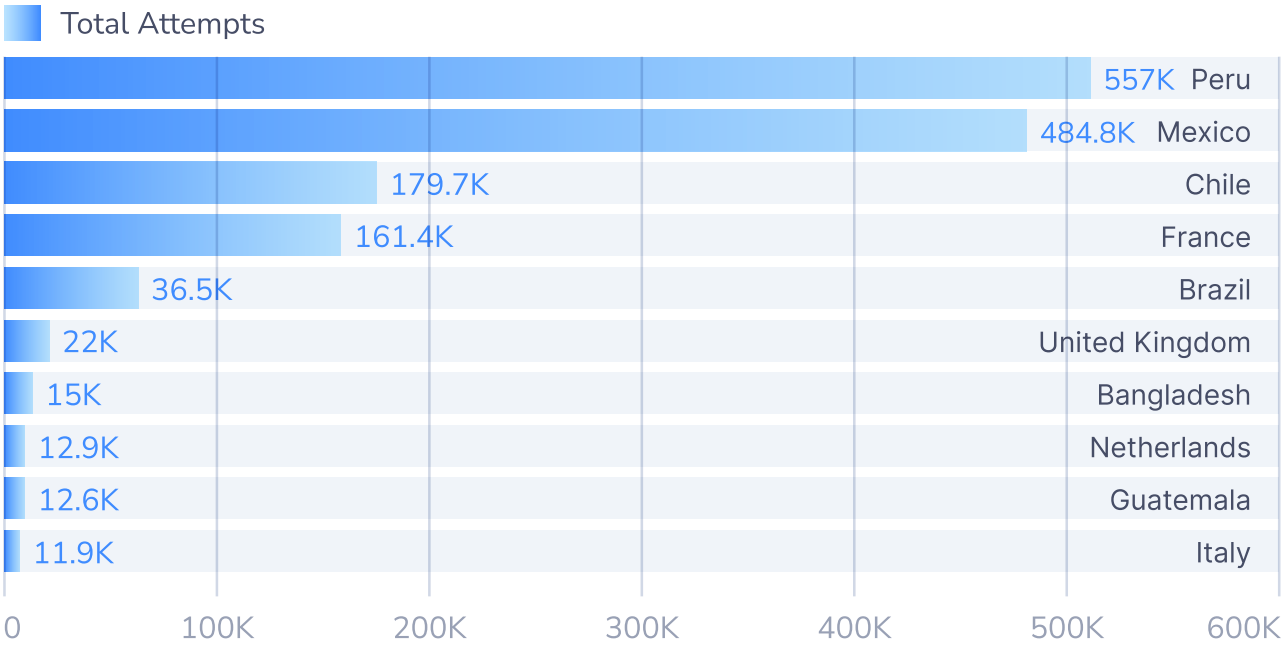
WHAT IT IS

This section identifies the top 10 countries where Flash Calls were received using local destination numbers, based on the number of alerted attempts during the quarter. A Flash Call with a local number occurs when a verification call is placed to a number that matches the local numbering format of the receiving country, making it harder to detect as foreign or suspicious. Fraudsters may exploit this method to evade international traffic filters, bypass fraud detection systems, and blend Flash Calls into regular traffic patterns.

Q3 HIGHLIGHTS

Top destinations with local numbers: Peru leads with an overwhelming 557K alerted attempts, followed by Mexico (484.8K) and Chile (179.7K).

TOP DESTINATIONS FOR FLASH CALLS WITH LOCAL NUMBERS



WHAT THE DATA TELLS US

Analysis of Q3 data reveals a clear and emerging trend in Flash Call activity involving local numbers, particularly in Peru and Mexico, with similar patterns also appearing in Chile and France. Fraudsters are increasingly reusing successful local-number spoofing strategies across multiple countries, generating Flash Calls that mimic domestic numbering formats to evade detection.

This indicates a replicable methodology, likely orchestrated by the same operators, that is now spreading to additional regions. Early signs suggest that countries such as Brazil, the UK, Bangladesh, the Netherlands, Guatemala, and Italy may also be targeted using the same local-number tactics. While these patterns are still developing, the data highlights the rapid adaptability of fraudsters and the need for proactive detection measures to prevent wider adoption.

COMMENTARY:

CLI SPOOFING: THE INVISIBLE ENGINE BEHIND MOST MODERN FRAUD

WHAT IT IS

CLI (Calling Line Identification) spoofing is the practice of falsifying the caller ID presented to the recipient of a call. Fraudsters manipulate the calling number to disguise their true identity or origin, making it appear as if a call is coming from a trusted source, a local number, or even a known contact.

Originally used to trick users into answering spam or Wangiri calls, spoofing has now evolved into a much more adaptive and complex fraud vector. It underpins much of today's call-based fraud ecosystem, silently enabling everything from missed-call scams to large-scale Flash Call operations.

Q3 HIGHLIGHTS

Local-number spoofing has surged, particularly in regions like Peru, Mexico, and Chile, where fraudsters are generating Flash Calls using local-looking CLIs.

Spoofed CLIs are increasingly being used for Wangiri attacks, masking international revenue-share numbers with domestic prefixes to trick subscribers into calling back.

Spam, scam, and robocall campaigns continue to rely on CLI rotation and spoofing to bypass blocking lists and appear more legitimate to users and networks.

WHAT THE DATA TELLS US

In Q3 2025, we're seeing a significant shift in how spoofing is being operationalized. Historically, spoofing served as a disguise, but now it's a weaponized automation tool. Fraudsters are using local-number spoofing to simulate Flash Calls that look entirely domestic, allowing them to blend verification traffic into standard call flows.

This approach is particularly dangerous because it:

- bypasses traditional anti-fraud rules that rely on international routing detection
- reduces consumer suspicion because the incoming number looks familiar
- overwhelms detection systems as millions of micro-duration calls are distributed across legitimate ranges

COMMENTARY:

CLI SPOOFING: THE INVISIBLE ENGINE BEHIND MOST MODERN FRAUD

In several customer networks, AB Handshake detected a repeating pattern where Flash Calls were generated using spoofed local CLIs, often mimicking nearby area codes or mobile prefixes. These were not isolated to one region but were seen across Latin America, Europe, and parts of Asia. The same operators appear to be recycling number pools and techniques from one geography to another, rapidly adapting as detection rules tighten.

THE LINK TO WANGIRI AND SPAM

It's becoming increasingly evident that the same technical infrastructure used for Wangiri and spam operations is now being repurposed for Flash Call activity. The spoofing logic that once focused on enticing callbacks now focuses on generating trust and avoiding detection. In effect, fraudsters' intent has evolved, but the underlying toolset (CLI spoofing) remains the same.

Wangiri attacks spoof to entice; flash calls spoof to disappear.

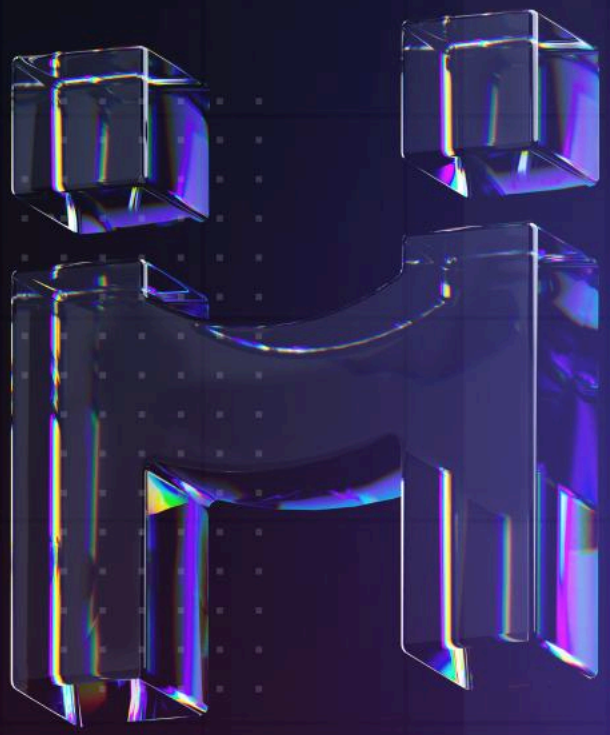
WHAT SUCCESS LOOKS LIKE AND HOW WE CAN GET THERE

Fraudsters have become adept at using spoofing dynamically, manipulating CLI data in real time to imitate local traffic and pass through filters. The traditional reliance on statistical or heuristic detection is no longer sufficient. Only real-time, cryptographically verified call validation can close this loophole.

That's where AB Handshake's Call Validation solution becomes critical. By enabling operators to verify every call between networks, confirming that both the A and B parties are legitimate and that the CLI has not been altered, AB Handshake's system makes CLI spoofing ineffective. When each call is validated through handshake-based cryptographic confirmation, spoofed identities simply fail the validation and are blocked before reaching the subscriber.

As fraudsters continue to innovate, so must we. AB Handshake's Call Validation solution offers a network-level truth layer that renders spoofing ineffective and restores confidence in caller identity across the telecom ecosystem.

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