AB HANDSHAKE

FRAUD REPORT

Q2 2025

ABHANDSHAKE.COM

Q2 2025

For AB Handshake customers, Q2 2025 has shown a bustling fraud landscape across voice and SMS. From classic IRSF and PBX hacks to Wangiri and the newer Wangiri 2.0 that targets enterprises, fraudsters continue to adapt.

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. Q2 2025 is interesting because we see the tried-and-true schemes still working - and some fraudsters becoming more strategic about who and when they attack.

Our Q2 review focuses on 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:

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 - A CLASSIC, BUT STILL EFFECTIVE

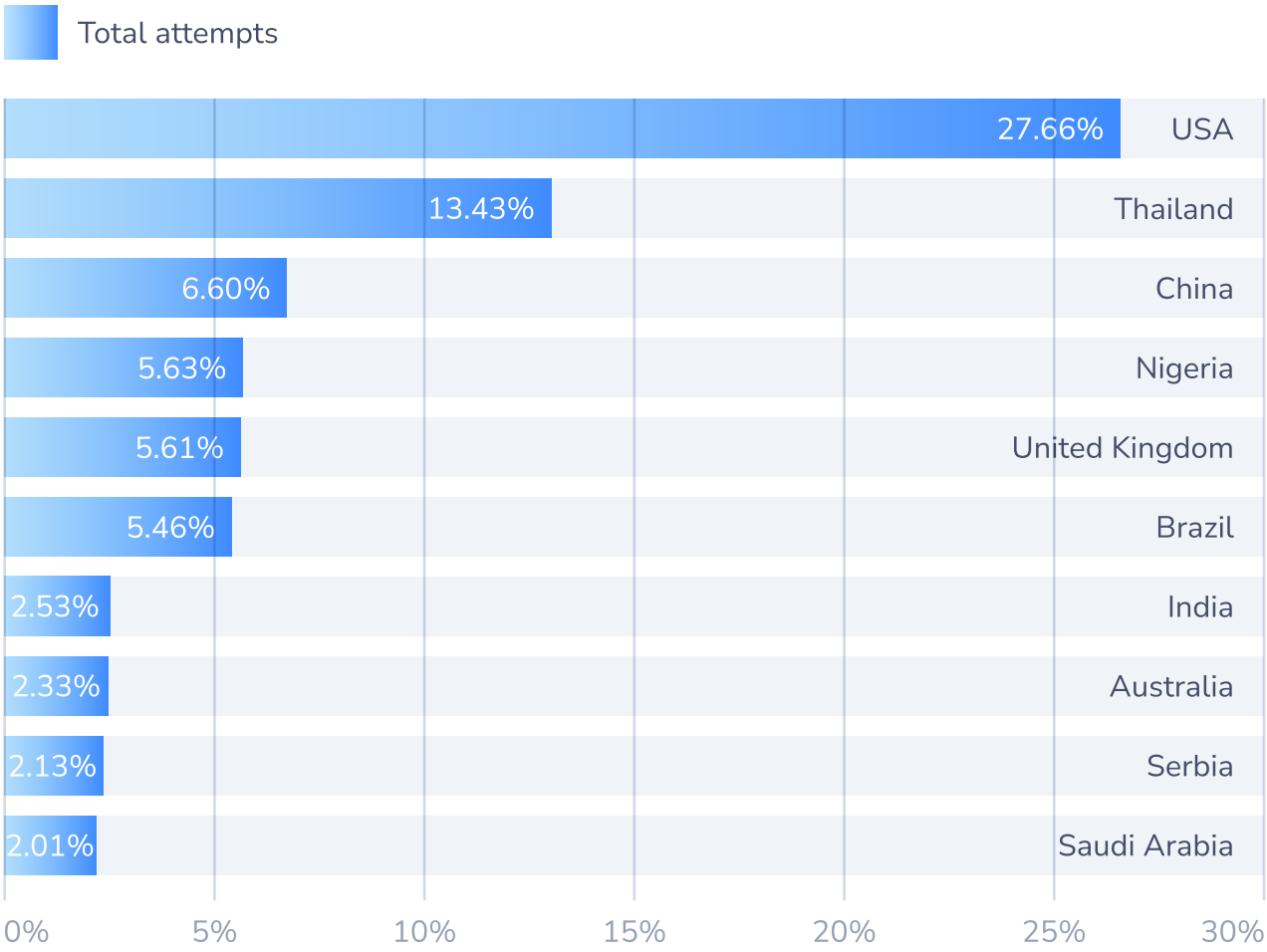
WHAT IT IS

IRSF is the artificial inflation of calls to revenue-share numbers. Fraudsters generate volume terminating to them in order to profit from a share of the call termination revenue.

Q2 HIGHLIGHTS

Top source (victim) ranges by share: USA (27.66%), Thailand (13.43%), and China (6.60%). These three alone approached half of observed IRSF traffic.

TOP 10 COUNTRIES BY IRSF ATTEMTS RELATIVE TO ALL IRSF ATTEMTS (ALL COUNTRIES)



IRSF - A CLASSIC, BUT STILL EFFECTIVE

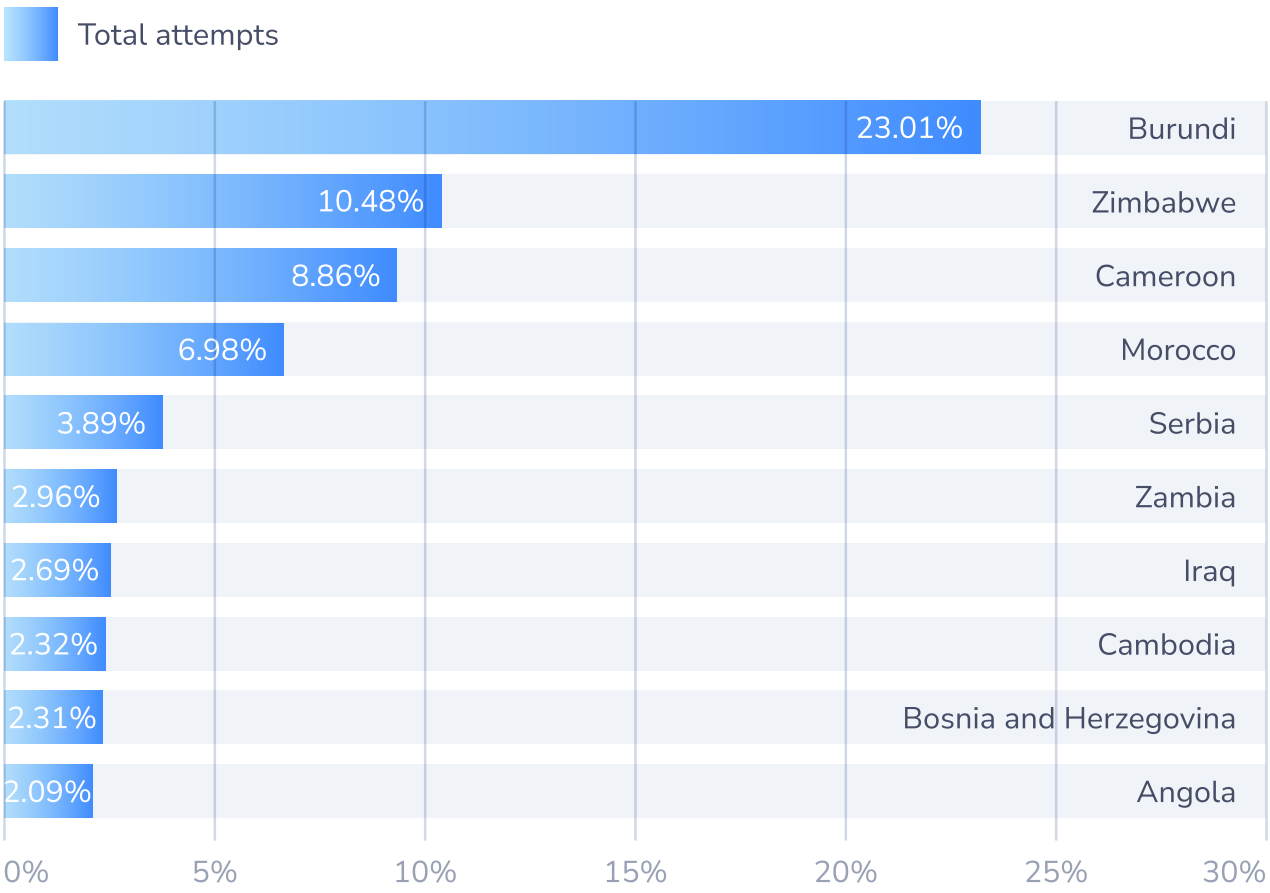
WHAT IT IS

IRSF is the artificial inflation of calls to revenue-share numbers. Fraudsters generate volume terminating to them in order to profit from a share of the call termination revenue.

Q2 HIGHLIGHTS

Top destination-associated ranges used to host IRSF numbers included Burundi (23.01%), Zimbabwe (10.48%), and Cameroon (8.86%).

TOP 10 EXPLOITED NUMBER RANGES RELATED TO COUNTRIES IN IRSF ATTEMPTS COMPARED TO ALL IRSF ATTEMPTS



IRSF - A CLASSIC, BUT STILL EFFECTIVE

WHAT THE DATA TELLS US

IRSF remains opportunistic: fraudsters combine easy-to-attain revenue-share numbers with ranges that have low legitimate traffic. That said, more sophisticated attacks hide in busier countries precisely because rising legitimate traffic forces FMSs to raise thresholds - which fraudsters exploit.

IRSF is one of the most common and expected types of all telecommunications fraud, and when it occurs, fraud professionals know it will not be the last time they see it.

Maybe your network saw its most recent IRSF event from a stolen phone, a hacked device like a PBX, or through subscription fraud.

Maybe that IRSF was pretty straightforward to identify and targeted common high-risk countries, or perhaps it used a more strategic approach to avoid detection by standard rules, such as changing patterns, switching target terminating B numbers, or using multiple calling numbers, for example.

As fraud professionals, we know IRSF as the artificial inflation of traffic towards a revenue-share number, where the fraudster generating those calls gains revenue.

We also know that fraud never stops, it only changes, but how much can IRSF really change?

There are many established high-risk ranges in the world that operators can keep up to date with, including revenue-share numbers that fellow operators have had IRSF generated to and have reported, for example GSMA's T-ISAC list. Theoretically, this allows operators to proactively block or at least watch for any traffic towards these numbers and get ahead of potential-revenue share fraud in any form.

While there will also be the odd IRSF attack targeting ranges in countries that are surprising (and probably short-stopped), how much do 'risky destinations' for IRSF truly change?

As you have seen, many of the top destinations in AB Handshake's Q2 2025 IRSF report are common on any high-risk number list and are not surprising to any fraud professional.

IRSF - A CLASSIC, BUT STILL EFFECTIVE

IRAQ AND THE PROBLEM WITH THRESHOLDS

Iraq appeared 7th among our top destination-associated ranges for IRSF. Even the most basic Fraud Management System (FMS) will treat many Iraqi number ranges as high-risk. This means any sizable traffic towards an Iraqi destination will likely trigger instant alerts on traffic terminating there, whether across a few calls or minutes. This approach is used to locate IRSF in easy-to-identify, high-risk locations where there is little daily traffic.

Interestingly, however, Iraq has in recent years become, to some extent, a destination for novel tourism. As more and more people visit Iraq, be it for business or adventure, calling patterns change, and those alert thresholds on traditional FMSs must change along with them.

The more legitimate traffic a very high-risk country receives day to day, the higher these call-count/duration thresholds need to be raised on any older, traditional FMS; otherwise, the fraud team will simply be faced with countless false-positive alerts.

Iraq, just like many countries in the world, is receiving more and more typical traffic, but also has these high-risk revenue-share ranges that are vulnerable to IRSF termination, so it needs to be managed carefully.

The question this raises is: how does a system user even begin to manage this?

The fraud analyst managing an FMS will certainly have noticed rising alert counts and increasing false-positive rates in this case, and they will also know something needs to be changed, but what? Do you increase the call-count thresholds, the total duration terminating towards a B number, or both? Do you increase them by 1, 10, 100, or 1000?

We also all know that global traffic patterns frequently change due to new businesses, global events, political developments, new conference call numbers, or, as in Iraq's case, tourism trends.

Standard rule- and threshold-based system approaches simply alert at low levels, as they must. However, this shows the true need for an AI-driven, machine-learning approach to detect the IRSF traffic within the legitimate traffic of a changing destination country.

AI is ideal for identifying anomalous traffic and key patterns when trained on example cases. IRSF is the perfect example use case where, if implemented correctly, AI can be trained to an extremely high level given enough data.

IRSF is also a type of fraud that can vary immensely from attack to attack and take many forms across different fraud methods used to complete it, such as Wangiri, Wangiri 2.0, and PBX hacking, to name a few. However, IRSF can also be easily identified no matter what the strategy, through signs such as automation, similar but not identical call durations, short, repeating, and possibly similar intervals between calls, simultaneous calls, high ASR (Answer-Seizure Ratio, indicating the percent of those calls that are connected), the time of the call (as fraudsters are banking on you being asleep and not

IRSF - A CLASSIC, BUT STILL EFFECTIVE

IRAQ AND THE PROBLEM WITH THRESHOLDS

watching your alerts at 3 am), and over 200 other features used by AB Handshake's AI Shield to detect this and other types of fraud.

Fraudsters are clever (most of the time... We have also previously spotted an IRSF fraudster taking a break from IRSF to call their bank for reasons that we can only guess where to check on their ill-gotten gains...). As shown by this case, fraudsters may also have identified this monitoring difficulty with countries just like Iraq, which is why they choose it as a destination for IRSF traffic.

Even a few years ago, choosing Iraq as the destination for your IRSF traffic would have been foolhardy, as it received so little traffic from most carriers that the traffic would have been instantly identified. Does this show us that even fraudsters can tell when thresholds just aren't working anymore and have to be raised on older, traditional FMSs?

Burundi, which was our most targeted country for IRSF in our Q2 2025 report, is exactly that. Burundi does not usually receive large amounts of traffic from international carriers and also contains established high-risk ranges for IRSF.

This shows us that these attackers have likely stumbled across a blind spot in another FMS and, after finding success, are reusing it elsewhere. Essentially, they are hoping their blind luck will pay off again with such a daring and easy-to-spot attack.

Fraudsters will often reuse the same IRSF ranges across regions and customers (hence GSMA's T-ISAC list can be very beneficial in warning future unsuspecting victims about ranges to watch out for). However, seeing IRSF like this in such an easy-to-find way means there is a carrier out there who probably suffered financially from the same attack previously.

So, how do you detect IRSF to a very high-risk country for fraud that also receives legitimate traffic without generating high alert counts? Easily. Do not rely on rules alone; they will not sustain you forever. Instead, start to learn the benefits of AI and machine learning detection. By relying on algorithms to identify suspicious patterns for you, in combination with manual alerts you wish to have, you can benefit from this approach.

PBX HACKING — THE TROJAN HORSE FOR IRSF

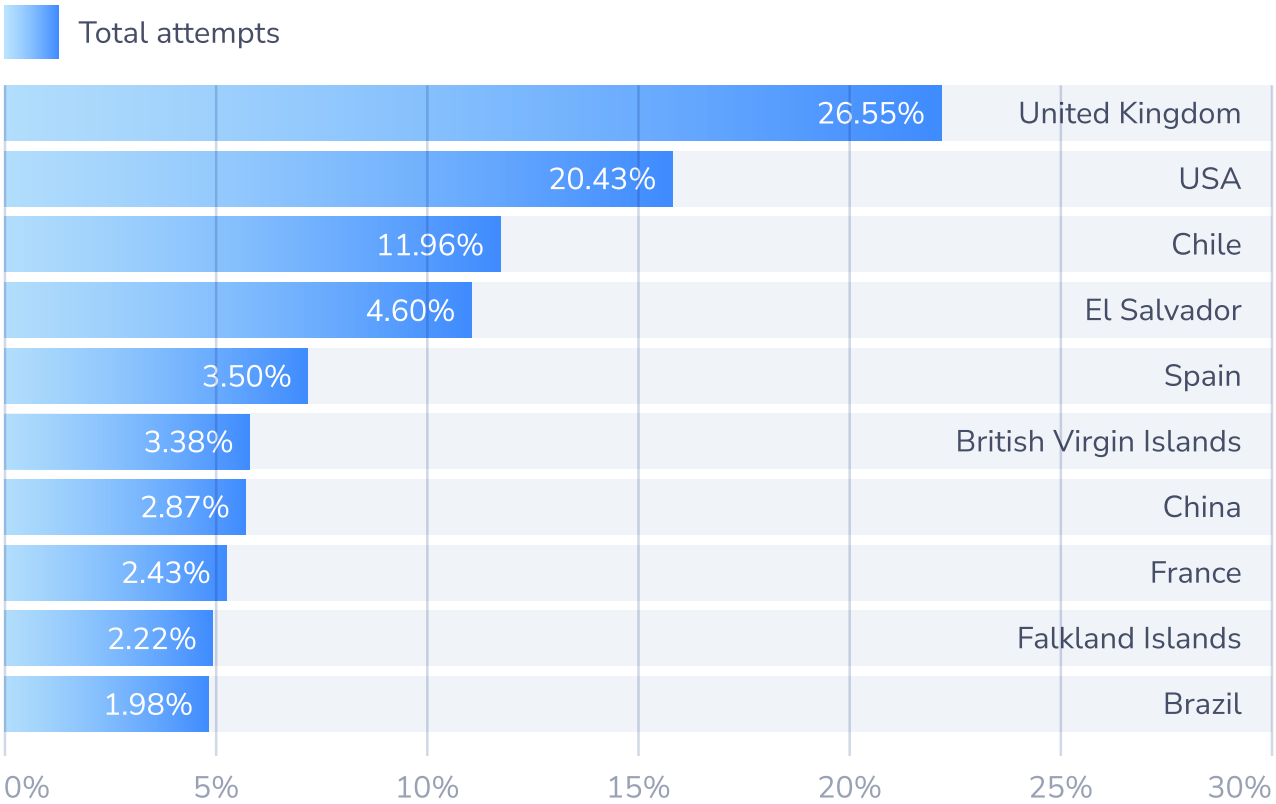
WHAT IT IS

A PBX device, often used by enterprise/business customers to manage their multiline systems, offers an easy attack avenue for fraudsters. Lax or sometimes absent security, such as weak or missing passwords or PINs on the device (think “1234”), enables fraudsters to access and misuse the PBX, turning it into a launching pad for mass international calls -often straight into IRSF.

Q2 HIGHLIGHTS

Top victim countries by share of PBX hacking attempts: UK (26.55%), USA (20.43%), and Chile (11.96%).

TOP 10 SOURCE COUNTRIES BY PBX HACKING ATTEMPTS RELATIVE TO ALL PBX HACKING ATTEMPTS (ALL COUNTRIES)



WHAT THE DATA TELLS US

PBX hacking continues to be a common method used to commit IRSF, combining security vulnerabilities, a lack of security awareness, and vulnerable access points for the generation of international calls.

WANGIRI - MISSED-CALL CALLBACK FRAUD, A CLASSIC

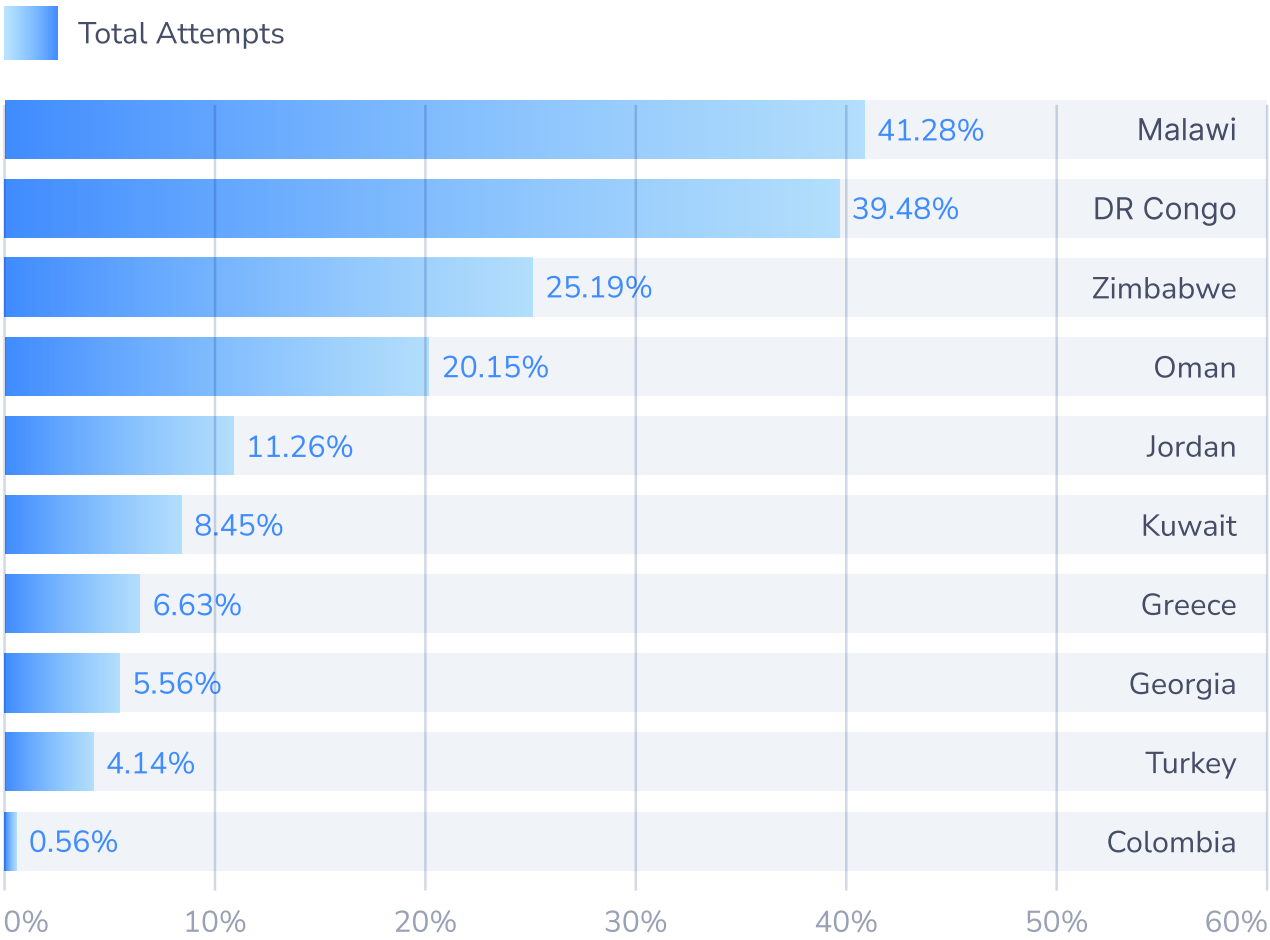
WHAT IT IS

Wangiri is a one-ring-and-cut scam that attempts to entice recipients to unknowingly call back a revenue-share number, allowing the fraudster to profit from the termination revenue.

Q2 HIGHLIGHTS

Top destination countries for return calls to Wangiri numbers: Malawi 41.28%, DR Congo 39.48%, Zimbabwe 25.19%, Oman 20.15%, Jordan 11.26%, Kuwait 8.45%, Greece 6.63%, Georgia 5.66%, Turkey 4.14%, and Colombia 0.56%.

TOP 10 DESTINATION COUNTRIES BY WANGIRI ATTEMPTS, RELATIVE TO TOTAL TRAFFIC TO EACH COUNTRY



WANGIRI - MISSED-CALL CALLBACK FRAUD, A CLASSIC

WHAT THE DATA TELLS US

Wangiri attacks continue to rise at alarming rates globally, with some countries reaching the point where almost half of their incoming terminating traffic is to revenue-share numbers.

There are many well-established high-risk countries that have been identified as being used to terminate IRSF calls following a Wangiri attack, most notably Malawi, the DR Congo, and Vietnam, to name a few.

Seeing such high rates of fraud terminating to high-risk countries like these reiterates our observation; that sometimes fraud is not new or strategic, that it can often simply occur exactly where you'd expect it, requiring a deft approach to detection, analysis, and blocking.

Success is not zero fraud overnight — it's making fraud unprofitable. By utilizing AI-driven detection and making well-considered decisions about which fraud management software to use, operators can drastically shrink the attack surface. Doing this is hard, but it doesn't have to be with a trusted, experienced partner like AB Handshake.

WANGIRI 2.0 — A SMARTER, ENTERPRISE-FOCUSED VARIANT

WHAT IT IS

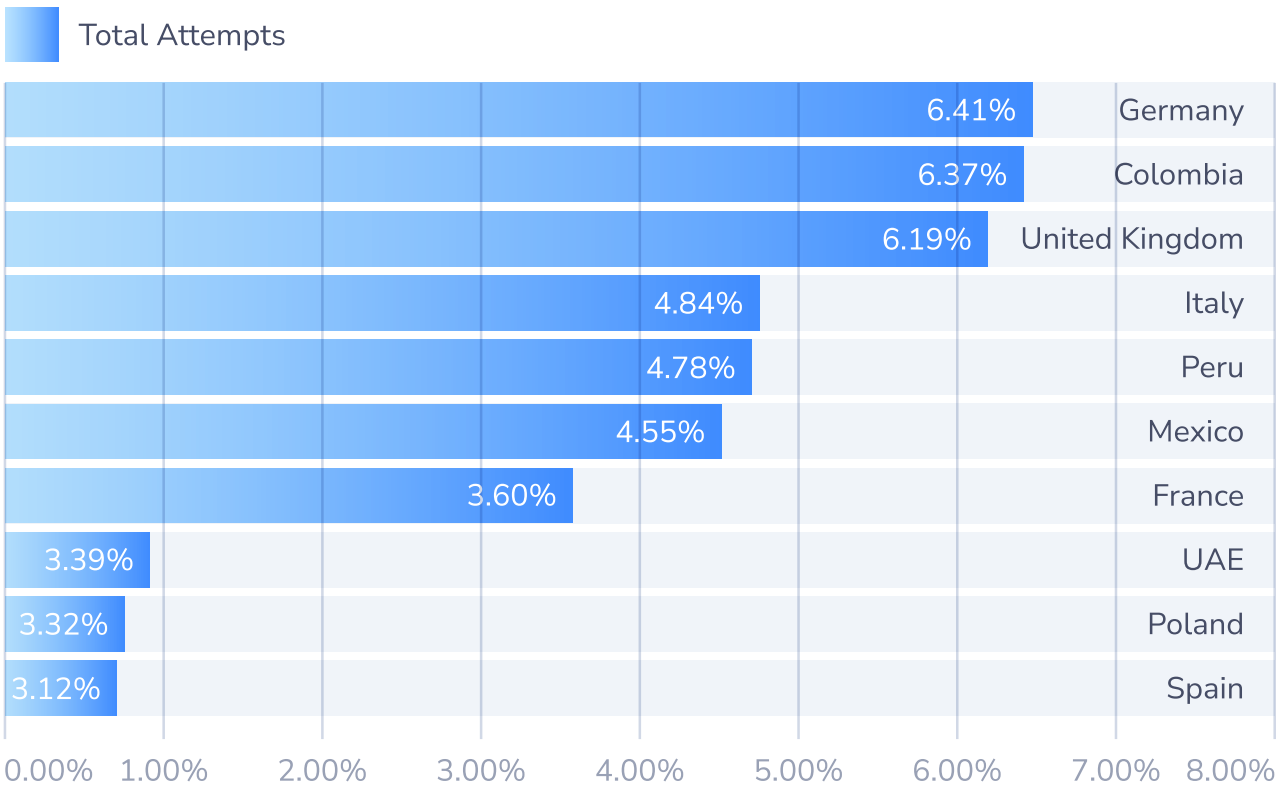
Wangiri 2.0 instructs bots to populate enterprise contact forms with revenue-share numbers or numbers that prompt callbacks (e.g., for one-time passwords). The enterprise then replies, often through expensive call centers or automated customer contact flows.

Enterprises, especially inbound sales teams, rely on callbacks; internal staff and automated workflows rarely validate numbers entered into customer forms. Fraudsters weaponize that trust — and the economic cost of a mistaken business callback is routinely higher than that of an individual subscriber callback.

Q2 HIGHLIGHTS

Top enterprise source countries receiving form-stuffed callbacks: Germany (6.41%), Colombia (6.37%), and the UK (6.19%).

TOP 10 SOURCE COUNTRIES BY WANGIRI 2.0 ATTEMPTS, RELATIVE TO ALL WANGIRI 2.0 ATTEMPTS



WANGIRI 2.0 — A SMARTER, ENTERPRISE-FOCUSED VARIANT

WHAT IT IS

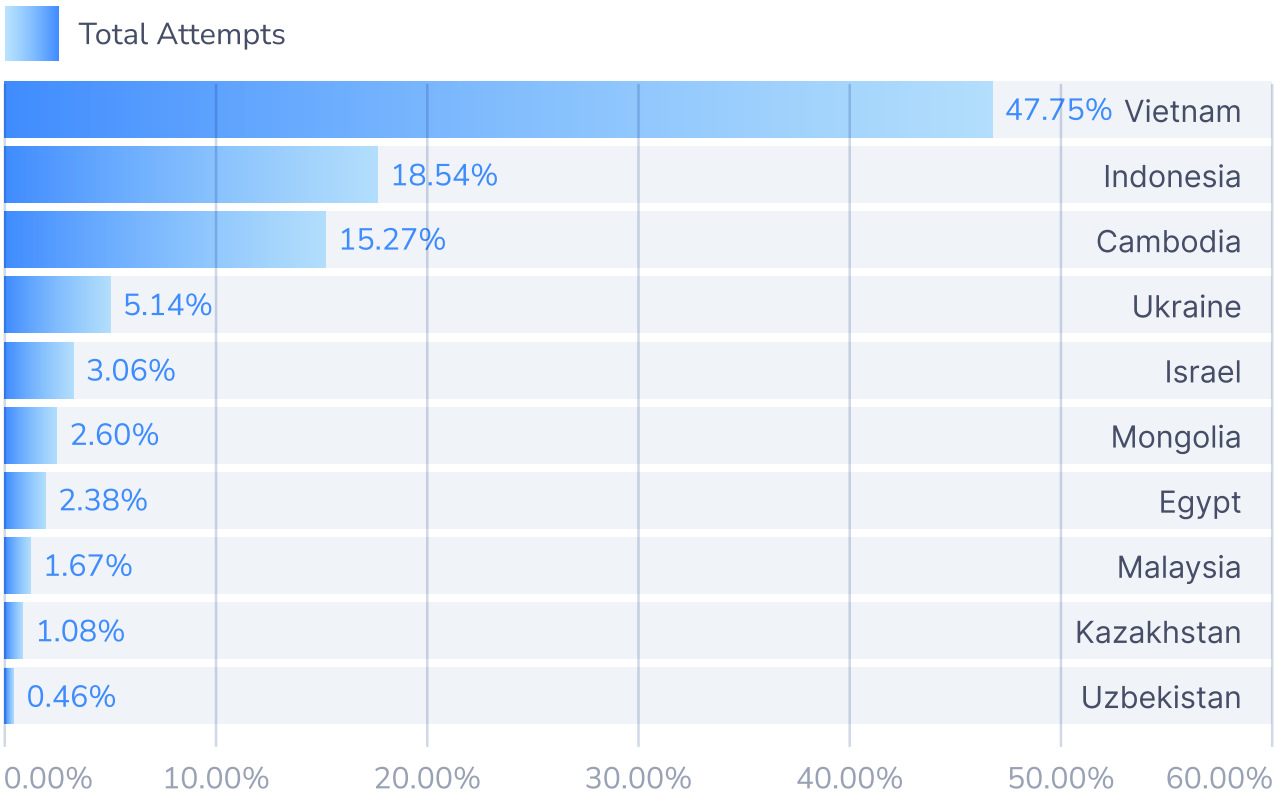
Wangiri 2.0 instructs bots to populate enterprise contact forms with revenue-share numbers or numbers that prompt callbacks (e.g., for one-time passwords). The enterprise then replies, often through expensive call centers or automated customer contact flows.

Enterprises, especially inbound sales teams, rely on callbacks; internal staff and automated workflows rarely validate numbers entered into customer forms. Fraudsters weaponize that trust — and the economic cost of a mistaken business callback is routinely higher than that of an individual subscriber callback.

Q2 HIGHLIGHTS

Revenue-share destinations that attackers used for callbacks: Vietnam (47.75%), Indonesia (18.54%), and Cambodia (15.27%). (Notably, some of these country codes closely resemble domestic ranges targeted by the enterprises.)

TOP 10 EXPLOITED NUMBER RANGES BY COUNTRY, RELATIVE TO ALL WANGIRI 2.0 ATTEMPTS



WANGIRI 2.0 — A SMARTER, ENTERPRISE-FOCUSED VARIANT

WHAT THE DATA TELLS US

Wangiri 2.0 is showing interesting attack vectors, with the top source countries being targeted at almost equal rates. Countries including Germany, the UK, and Colombia, all of which have large-scale call centers and enterprise hubs, are being targeted at similar levels to trick and trigger call backs to revenue-share numbers.

FLASH CALLS — THE SILENT, UNMONETIZED 2FA LOOPHOLE

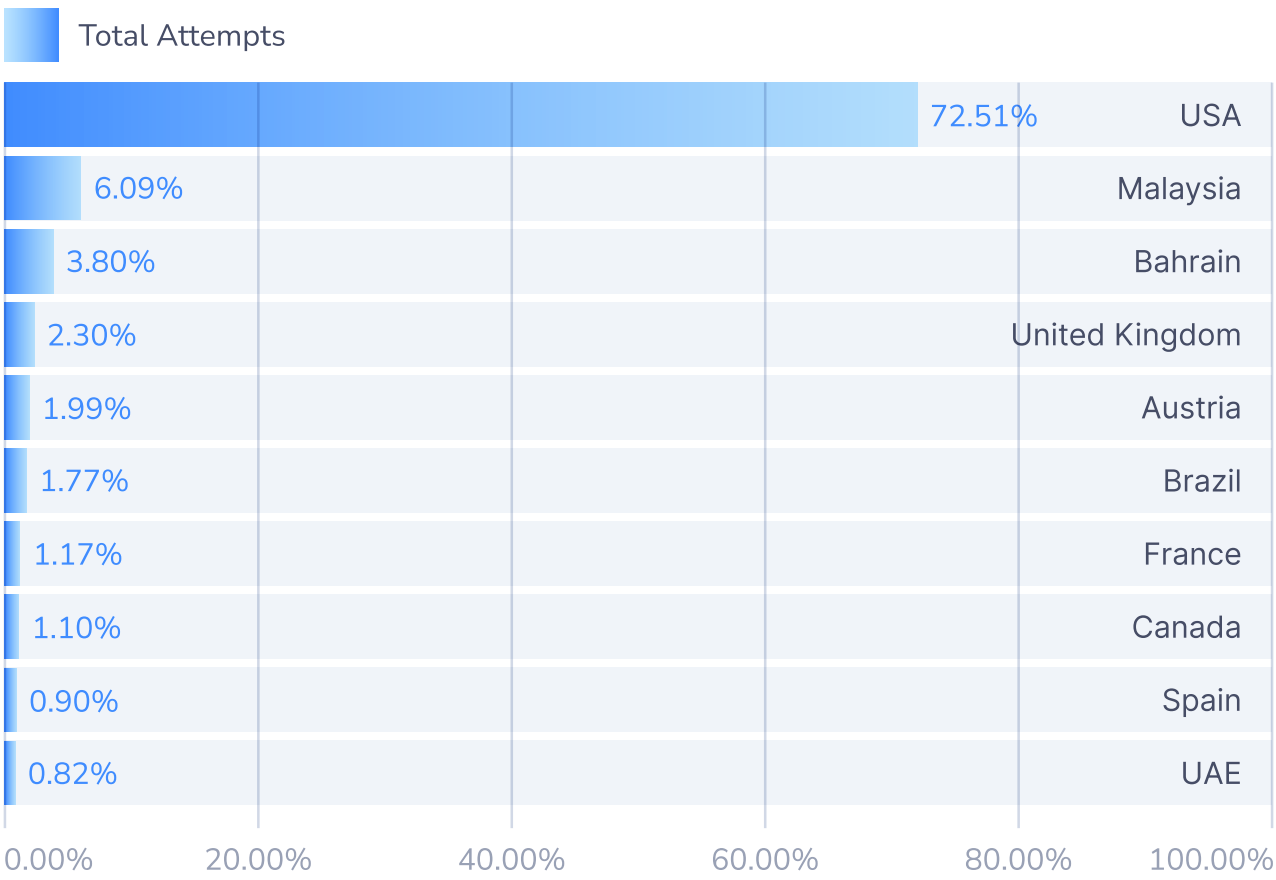
WHAT IT IS

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.

Q2 HIGHLIGHTS

US-associated number ranges dominated as the source for Flash Calls (72.51% of Flash Call traffic observed).

TOP 10 EXPLOITED NUMBER RANGES BY COUNTRY, RELATIVE TO ALL FLASH CALL ATTEMPTS



FLASH CALLS — THE SILENT, UNMONETIZED 2FA LOOPHOLE

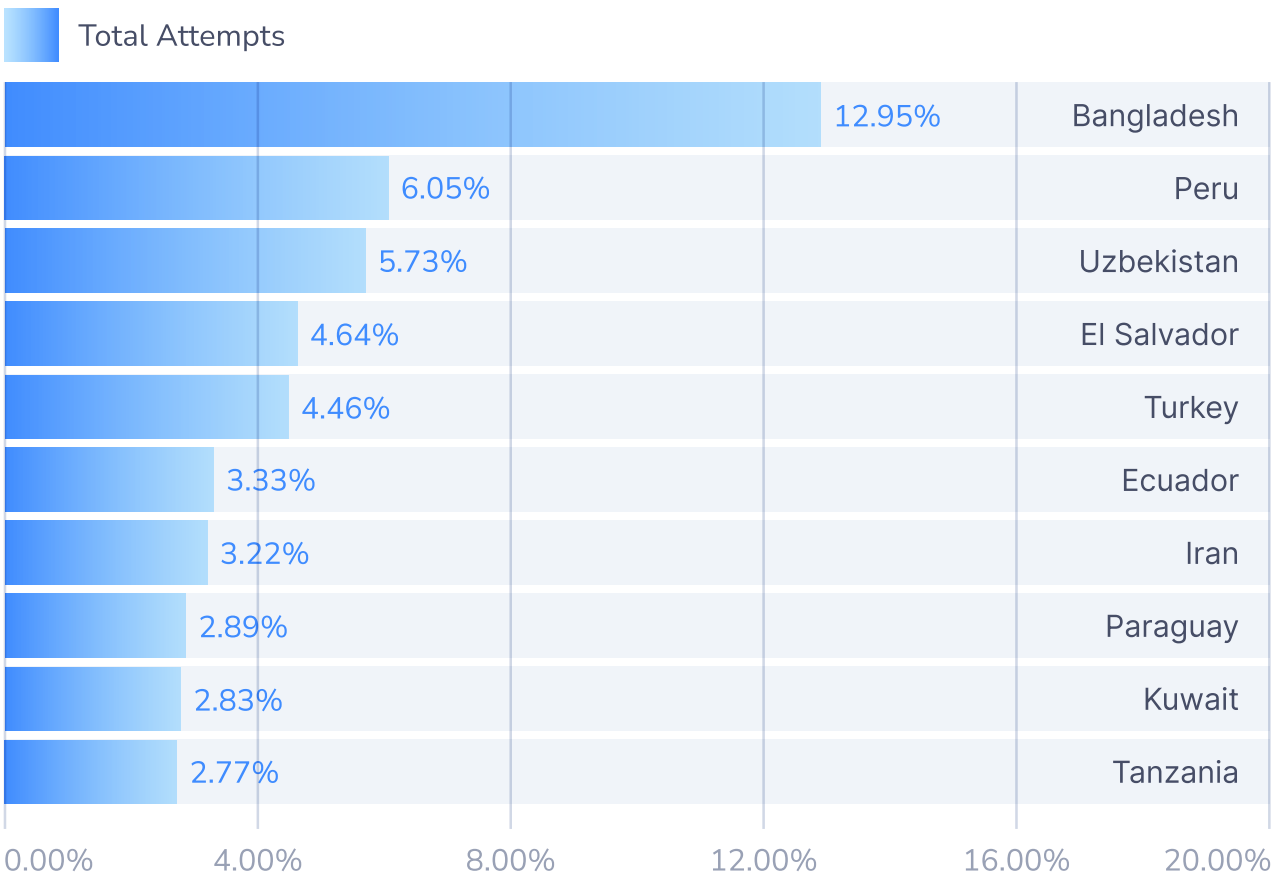
WHAT IT IS

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.

Q2 HIGHLIGHTS

Destination ranges most targeted included Bangladesh (12.95%), Peru (6.05%), and Uzbekistan (5.73%).

TOP 10 DESTINATION COUNTRIES BY FLASH CALL ATTEMPTS, RELATIVE TO ALL FLASH CALL ATTEMPTS



FLASH CALLS — THE SILENT, UNMONETIZED 2FA LOOPHOLE

WHAT THE DATA TELLS US

Flash Calls, a relatively new development in recent years, are continuing at enormous and unhindered levels. AI Shield's detections in this case show that many are originating from mainly US numbers, truly highlighting the messaging business's dramatic shifts. We also see the use of Flash Calls for authentication services being utilized by subscribers across the globe, with Bangladesh, Peru, and Uzbekistan among the highest consumers of the service.

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