AB HANDSHAKE

FRAUD REPORT

Q2 2026

ABHANDSHAKE.COM

Q2 2026 FRAUD REPORT — WHAT AB HANDSHAKE DATA REVEALS

Telecom fraud rarely follows a single pattern. The same traffic indicator can mean different things depending on the fraud type, market, and behavior behind it.

Our Q2 2026 Fraud Overview looks at the fraud activity observed across our customer environments during the quarter, covering IRSF, PBX Hacking-led IRSF, P2S, Wangiri and Wangiri 2.0, Spam and Scam calls, Flash Calls, and SMS AIT.

The data highlights how different these patterns can be. In some cases, fraud represented an exceptionally high share of observed traffic: Wangiri reached 99% of monitored traffic toward Zimbabwe and 98% toward Lesotho. In others, the challenge was distinguishing abuse from legitimate high-volume activity. Flash Calls, for example, generated 116 million termination attempts in the UK and 113 million in Bangladesh during this period.

The report also shows how telecom fraud increasingly intersects with digital services and the wider fraud ecosystem. P2S and Wangiri 2.0 can begin with the abuse of legitimate online workflows before appearing as telecom traffic, while spam and scam calls may be only the first step in a broader fraud chain that ultimately leads to financial loss elsewhere.

One theme runs through the Q2 data: volume or destination alone rarely tells the whole story. Understanding changes in traffic behavior, calling patterns, and the context surrounding individual communications is becoming increasingly important for distinguishing legitimate activity from emerging fraud.

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:

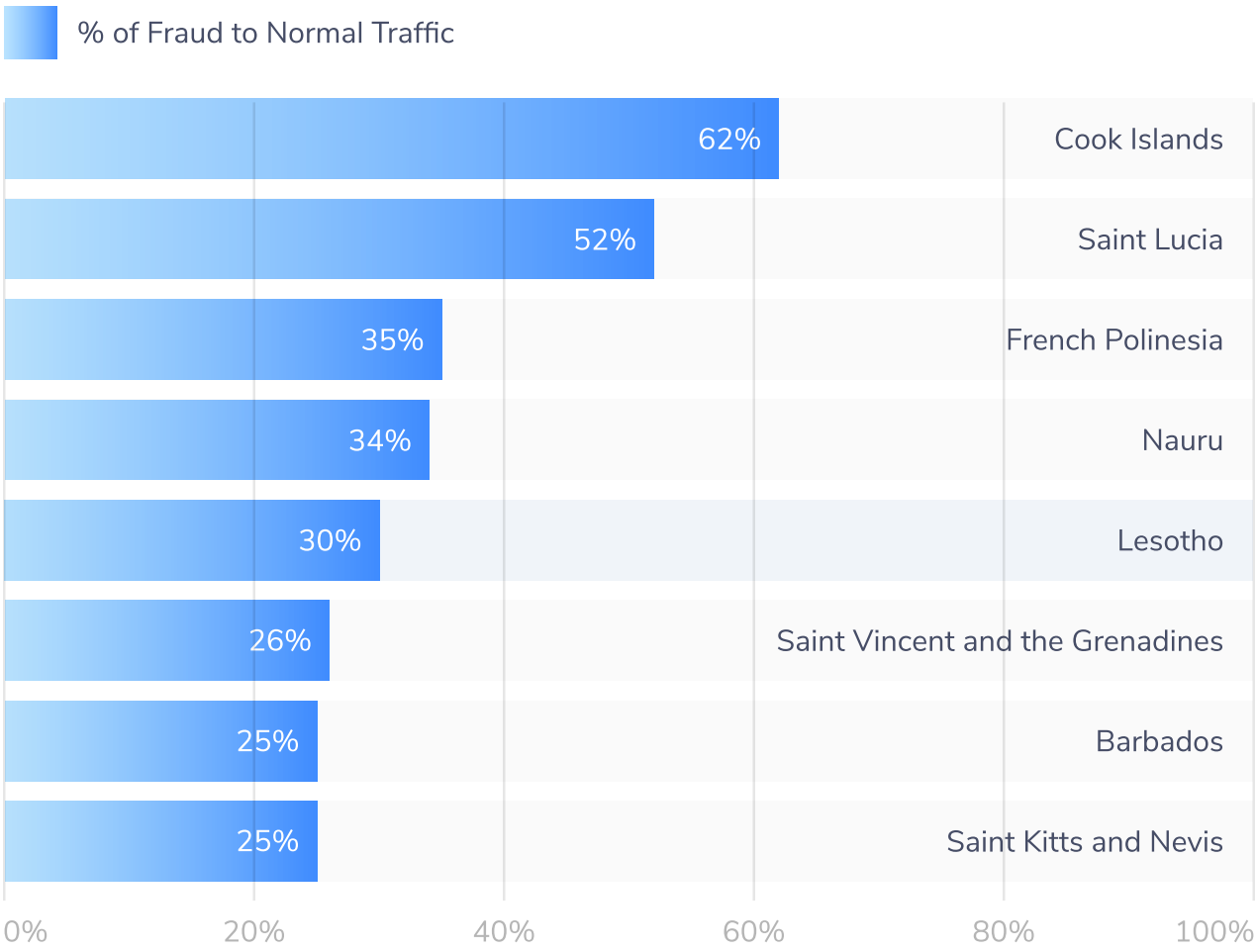
Subscribe

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.

This section presents the top 8 country range codes where IRSF (International Revenue Share Fraud) traffic had the highest ratio compared to legitimate (normal) traffic.

TOP FRAUD DESTINATIONS - % FRAUD



IRSF

WHAT THE DATA TELLS US

The high IRSF ratios for destinations such as the Cook Islands, Saint Lucia, French Polynesia, and Saint Vincent and the Grenadines demonstrate how fraudulent activity can represent a significant proportion of traffic even in smaller destination markets. These destinations may receive lower overall traffic volumes from AB Handshake customers, meaning that concentrated IRSF activity can have a disproportionately large impact on the traffic profile.

The Cook Islands recorded a particularly high fraud ratio of 62%, followed by Saint Lucia at 52%, and French Polynesia at 35%. Saint Vincent and the Grenadines also recorded a significant ratio of 26%. Locations such as the Cook Islands, Saint Lucia, and French Polynesia demonstrate that smaller destination markets can experience substantial levels of fraudulent traffic relative to their normal activity.

This pattern highlights the importance of monitoring fraud ratios alongside absolute traffic volumes using intelligent, context-aware methods rather than simply relying on high thresholds alone. A destination does not need to be a major international traffic hub for IRSF activity to become significant. Where legitimate traffic volumes are smaller, concentrated fraudulent activity can quickly represent a large proportion of the overall traffic and therefore become an important indicator of potential abuse. However, other factors should also be considered before alerting on such activity.

Another important consideration is that elevated fraud ratios should not be interpreted in isolation as evidence that a destination itself is inherently high-risk. IRSF campaigns can shift rapidly between destinations as fraudsters adapt routes, pricing, and revenue-share opportunities. The more valuable signal is therefore the deviation from an operator's expected traffic behavior: sudden changes in call volumes, destination mix, calling patterns, or the concentration of activity can indicate an emerging campaign even when the destination would not ordinarily be considered unusual. This reinforces the importance of contextual, behavior-based detection rather than relying solely on static destination-based rules.

This is why operators increasingly rely on advanced fraud management platforms such as AB Handshake's AI Shield, which can identify unusual IRSF patterns in real time and help detect emerging fraud activity before it develops into significant financial exposure.

PBX HACKING-LED IRSF

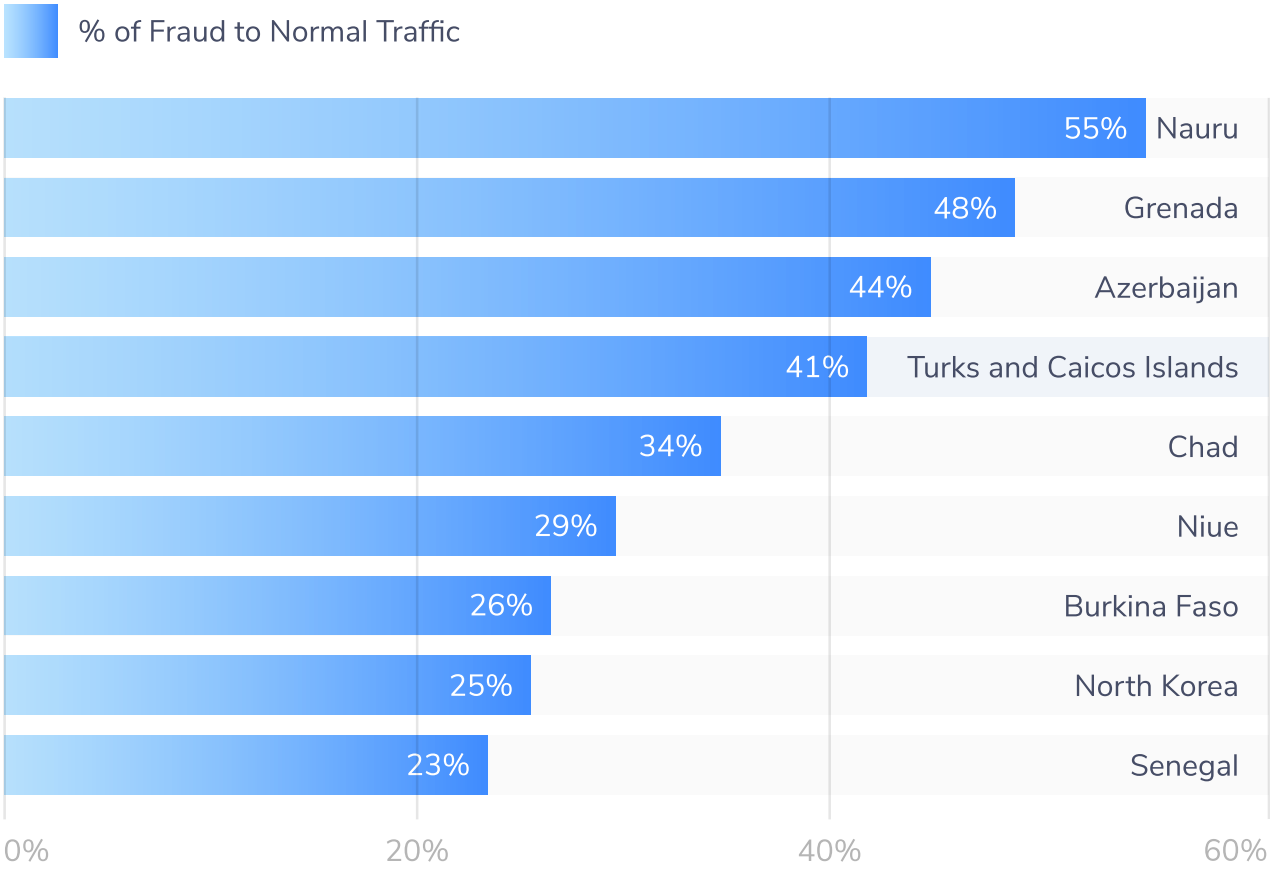
UNDERSTANDING IRSF TRAFFIC AND PBX HACKING METHODS

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).

The following dashboard identifies the top 9 country ranges where PBX hacking traffic had the highest ratio compared to normal (legitimate) traffic during the quarter.

TOP FRAUD DESTINATIONS - % FRAUD



PBX HACKING-LED IRSF

WHAT THE DATA TELLS US

Four destinations recorded fraud-to-normal traffic ratios above 40%, with Nauru leading at 55%, followed by Grenada at 48%, Azerbaijan at 44%, and the Turks and Caicos Islands at 41%. This represents a particularly strong concentration of PBX-related fraudulent activity, with a substantial proportion of observed traffic to each of these destinations identified as fraudulent.

The relatively small difference between the leading destinations is also notable. Rather than a single destination accounting for the majority of the activity, the data shows a cluster of four destinations where PBX fraud represents a similarly significant share of traffic. The gap between Nauru and Turks and Caicos Islands is only 14 percentage points, showing that the elevated PBX signal remains consistently strong across this group.

Importantly, PBX hacking differs from ordinary enterprise outbound traffic because the fraud requires unauthorized access to the enterprise's PBX system in the first place. Once that access has been obtained, fraudsters can use the compromised system to generate international calls, usually toward revenue-share destinations. This means that the presence of uncharacteristic outbound international traffic alone is not enough to identify PBX fraud; the behavior and characteristics of the calls provide the critical distinction.

The Q2 data also shows why those patterns matter: PBX hacking can manifest through specific calling behaviors associated with compromised business systems, allowing fraudulent activity to be distinguished from legitimate enterprise calling. In the underlying PBX fraud model, call timing is particularly relevant: traffic may be generated during business hours to avoid attracting attention from employees, or outside business hours when legitimate users are less likely to notice unusual activity. These behavioral signals help differentiate an apparently normal outbound enterprise call from traffic generated through a compromised PBX.

A further challenge with PBX-related fraud is that the compromise itself may remain invisible while the resulting traffic initially appears operationally legitimate. Because calls are generated through an authorized enterprise system, the fraud is not necessarily identifiable through the existence of international traffic alone. Detection therefore depends on understanding changes in the behavior of the PBX environment over time, such as unusual shifts in calling patterns, destinations, or activity relative to the organization's established baseline. This makes context particularly important: the same call pattern may be normal for one enterprise but highly anomalous for another.

PBX HACKING-LED IRSF

The remaining destinations continue to show fraudulent traffic, ranging from 34% in Chad to 23% in Senegal. Even at the lower end of the chart, almost a quarter of observed traffic is identified as fraudulent. This reinforces the notion that PBX fraud is not simply a question of identifying a handful of extreme destinations. Understanding the underlying calling behavior is essential to identifying where legitimate enterprise traffic ends and compromised PBX activity begins.

This is where advanced fraud management becomes particularly important. AB Handshake's AI Shield can analyze traffic behavior continuously, helping operators distinguish legitimate traffic from unusual calling patterns associated with compromised PBX systems and identify anomalous activity as it emerges.

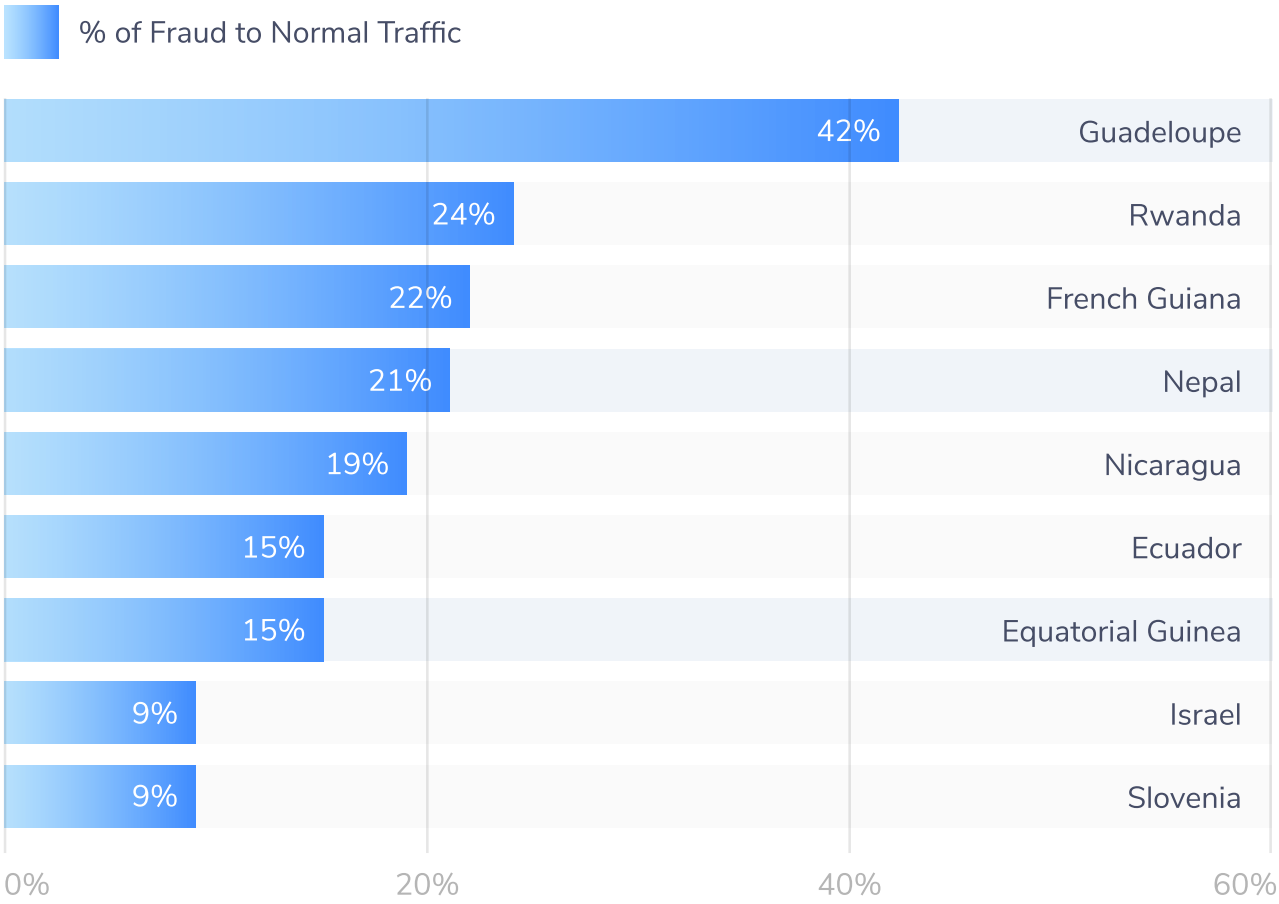
P2S FRAUD

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.

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

TOP FRAUD DESTINATIONS - % FRAUD



P2S FRAUD

WHAT THE DATA TELLS US

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. The repeated automated attempts generated by these systems can create distinctive patterns, with particular destinations becoming hotspots for this type of revenue-share fraud.

The data highlights an important characteristic of P2S: legitimate verification traffic can itself become a fraud vector when it is abused at scale. Voice OTP calls are designed to support genuine authentication processes, but automated systems can repeatedly trigger those processes without a legitimate user behind them. The resulting calls may therefore look like normal verification traffic at an individual level, while collectively forming a systematic pattern of fraudulent activity.

This also places P2S at an interesting boundary between application-level and telecom fraud. The attack can begin with a bot interacting with an online form or verification process, while the monetization occurs through the resulting telecommunications traffic to revenue-share numbers. The telecom traffic is therefore the visible consequence of an abuse mechanism that may have originated outside the telecom network itself.

The destination data supports this broader pattern. Guadeloupe recorded a 42% fraud-to-normal traffic ratio, while Rwanda, French Guiana, Nepal, and Nicaragua also recorded elevated ratios of 24%, 22%, 21%, and 19% respectively. Rather than indicating that these destinations themselves are necessarily the source of the attacks, the pattern shows where the resulting P2S traffic is becoming particularly concentrated.

This is what makes P2S different from more conventional forms of telecom fraud: the fraudster can exploit a legitimate digital service and its automated verification process, effectively turning that service into a mechanism for generating monetizable telecom traffic. Detecting the abuse therefore requires more than simply identifying whether an individual OTP call looks legitimate; it requires recognizing the repeated and systematic behavior surrounding those calls.

A key challenge with P2S fraud is that the telecom network may only see the final outcome of an attack that began elsewhere. The initial abuse can occur at the application or digital service layer, where automated systems repeatedly trigger verification processes, while the resulting voice traffic appears downstream as a series of legitimate-looking calls. This creates a visibility gap between the point of attack and the resulting telecom activity, making it particularly important to analyze patterns across the full sequence of events rather than assessing individual calls in isolation.

AB Handshake's AI Shield helps operators detect P2S fraud by identifying abnormal patterns of behavior across otherwise legitimate-looking traffic. AI Shield can help identify P2S activity by detecting behavioral patterns associated with automated or anomalous traffic, even where activity appears legitimate.

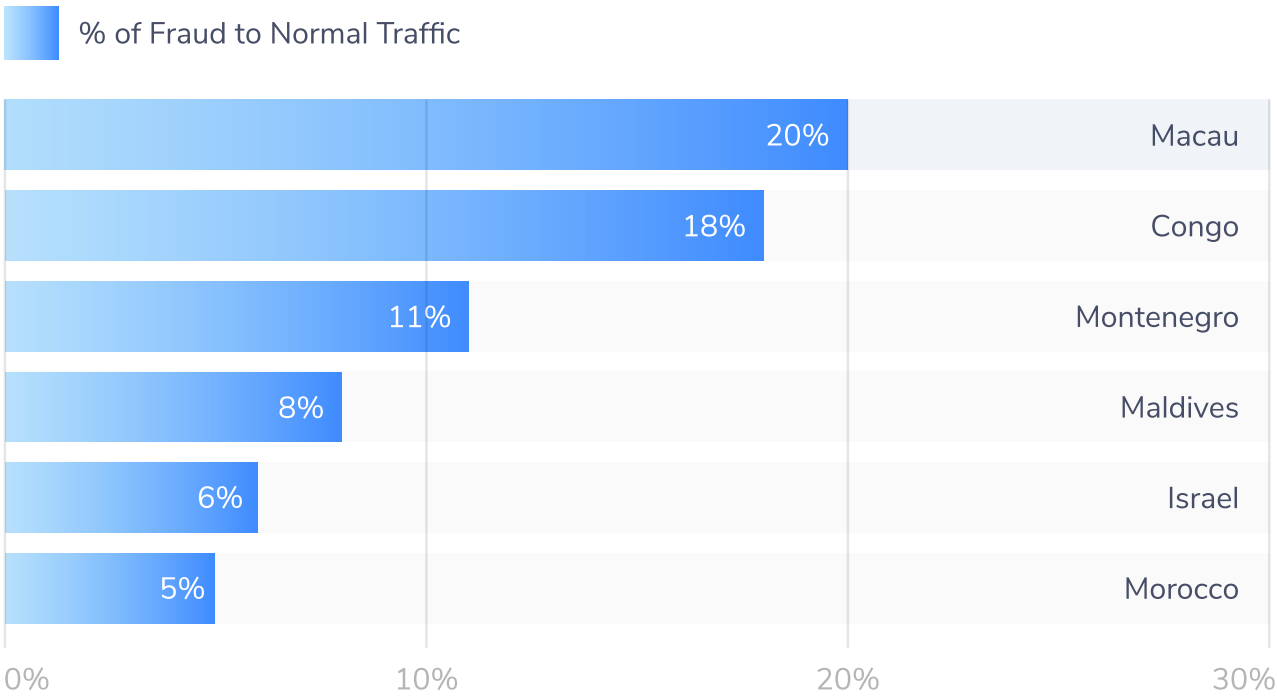
WANGIRI 2.0

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.

This section displays the top 6 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

WHAT THE DATA TELLS US

Wangiri 2.0 typically involves automated systems or bots that submit revenue-share numbers through online forms, triggering automated callbacks from enterprises or applications. Unlike traditional Wangiri, where the fraudster relies on an individual subscriber noticing and returning a missed call, Wangiri 2.0 can exploit an automated system to generate the callback itself.

This makes Wangiri 2.0 particularly interesting because the attack can begin outside the telecom network. A fraudster may interact with a legitimate online form or application, but the resulting action is a telecommunications event. The Q2 data illustrates this across a range of destinations. Macau recorded the highest fraud-to-normal traffic ratio at 20%, followed by Congo at 18%, while Montenegro was recorded at 11%. Maldives, Israel and Morocco also appear in the leading destinations at 8%, 6% and 5% respectively. The spread is notable because the destinations themselves are varied, reinforcing the notion that the underlying mechanism is not dependent on one particular geographic market.

The important distinction is therefore between the destination of the call and the mechanism that generated it. A callback to one of these destinations may appear, in isolation, to be a legitimate international call generated by an enterprise or application. It is the surrounding behavior that can reveal the fraudulent pattern.

The automation involved in Wangiri 2.0 also changes the economics of the attack. Rather than relying on individual subscribers making a decision to return a missed call, the fraudster can abuse automated enterprise or application workflows to generate callbacks at scale. This can make the activity more repeatable and less dependent on human behavior, while potentially allowing fraudulent traffic to be generated rapidly through systems that were designed to serve legitimate customers.

Wangiri 2.0 therefore, sits at an increasingly important intersection between application abuse and telecom fraud. The attacker does not necessarily need to compromise a telecom subscriber or directly manipulate the network. Instead, they can abuse a legitimate digital workflow and use the resulting telecom functionality to generate revenue. This makes behavioral analysis particularly important, as the individual call may look legitimate while the sequence of events surrounding it reveals the fraud.

This is where AB Handshake's AI Shield can provide an important layer of protection, combining advanced behavioral analysis with real-time fraud intelligence to identify unusual calling patterns and help operators detect Wangiri 2.0.

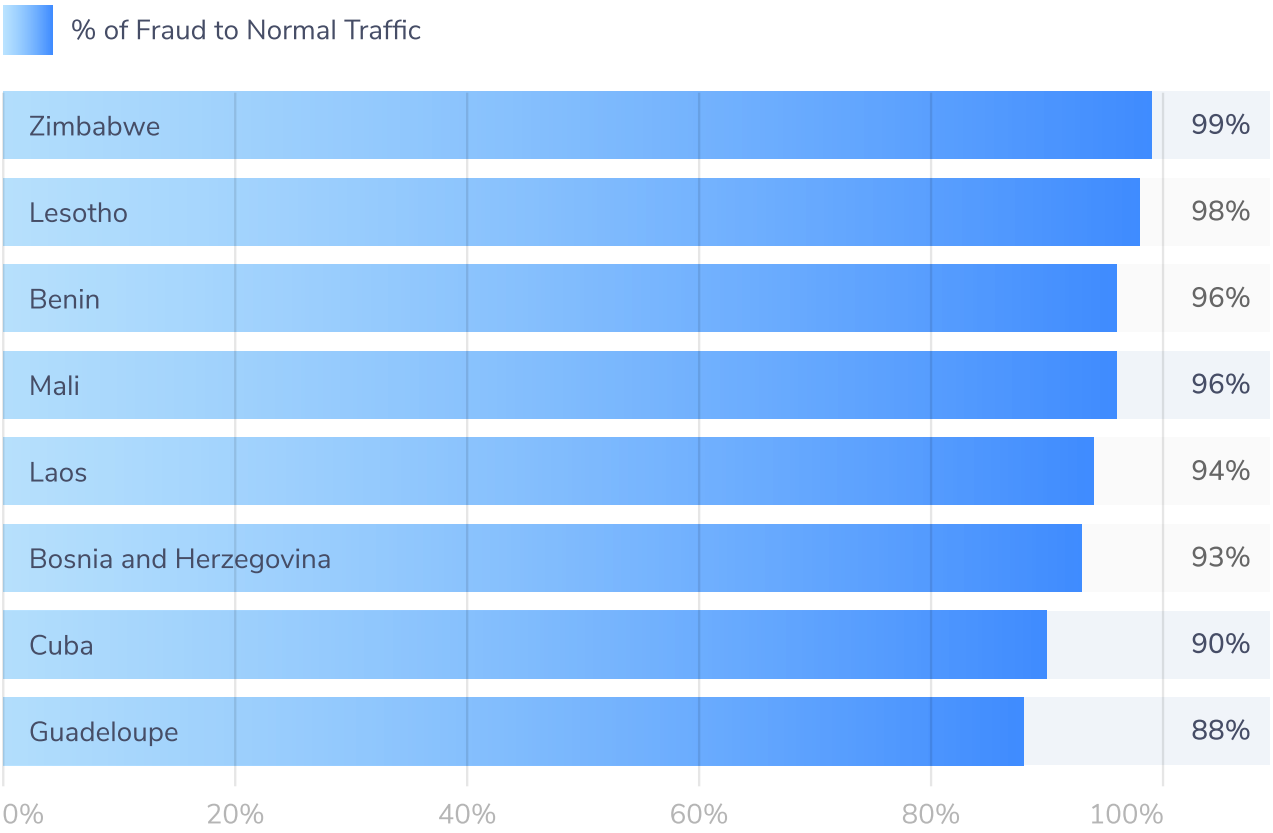
WANGIRI

UNDERSTANDING WANGIRI

Wangiri fraud works by triggering short one-ring calls or missed calls to users from revenue share numbers, enticing innocent subscribers to call back. Those who do return these calls do not realize they are calling a revenue share number that the fraudster is generating profit from calls to. Other means may be done to entice the caller to stay connected on the line for longer, such as recordings of a phone ringing out, or a long voicemail, etc.

The following dashboard identifies the country ranges with the highest counts of inbound Wangiri attack calls.

TOP FRAUD DESTINATIONS - % FRAUD



WANGIRI

WHAT THE DATA TELLS US

Wangiri fraud shows an extraordinary concentration of fraudulent traffic across the leading destinations in the Q2 data. Zimbabwe recorded a fraud-to-normal traffic ratio of 99%, followed by Lesotho at 98%, Benin and Mali at 96%, and Laos at 94%. At these levels, fraudulent traffic is not simply a noticeable component of the overall traffic profile; it represents almost all of the traffic observed toward these destinations.

The concentration remains exceptionally high across the rest of the list. Bosnia and Herzegovina recorded 93%, while Cuba reached 90%, and Guadeloupe recorded 88%. Even the lowest ratio shown therefore, indicates that the overwhelming majority of the traffic identified within these destination ranges was associated with Wangiri activity.

This is particularly significant because Wangiri is a relatively simple form of fraud that relies on a very ordinary piece of subscriber behavior. Fraudsters place short or one-ring calls to encourage recipients to call back, with those return calls connecting to revenue-share numbers from which the fraudster can generate revenue. The data shows how powerful that simple mechanism can become once an attack is established.

The extreme concentration of Wangiri activity also demonstrates how quickly a simple social-engineering technique can become highly efficient when deployed at scale. The underlying action required from the victim is as simple as returning a missed call, but once a campaign gains traction the same mechanism can be repeated across large numbers of subscribers. This makes Wangiri particularly dependent on rapid identification and response, as the value of the campaign may be generated before individual subscribers or operators recognize the broader pattern.

The geographic spread is also notable. The destinations represented here span multiple regions, including Africa, Asia, Europe, and the Caribbean. This suggests that the underlying opportunity is not tied to one particular market or geography. Instead, the common factor is the ability to exploit the callback behavior of subscribers and route those callbacks toward revenue-share numbers.

It is also important to understand these figures in the context of the different levels of visibility available across AB Handshake's customer base. AI Shield supports a variety of protection and integration models: for some customers, AB Handshake may see international interconnect traffic; others provide broader traffic visibility, real-time signaling data, or CDRs. This range of deployments gives AB Handshake exposure to fraud patterns emerging across different networks and markets, while also providing individual insight into how those attacks manifest within particular customer environments.

WANGIRI

As a result, a 99% fraud ratio can be seen as a strong signal within the traffic visible to the system, rather than suggesting that every call made to any one country is inherently fraudulent. The figure reflects the traffic and visibility available within the relevant monitored environment. The value of having such a broad range of customer deployments is that individual observations can contribute to a wider understanding of global fraud trends, while the same intelligence can be used to identify unusual behavior specific to an individual network.

This breadth of visibility is one of the strengths of AB Handshake's AI Shield. By combining different sources of network intelligence with AI-driven detection, the platform can identify unusually concentrated fraud patterns such as these and help operators distinguish genuine Wangiri activity from normal international traffic, providing the visibility and response capabilities needed as campaigns emerge and evolve.

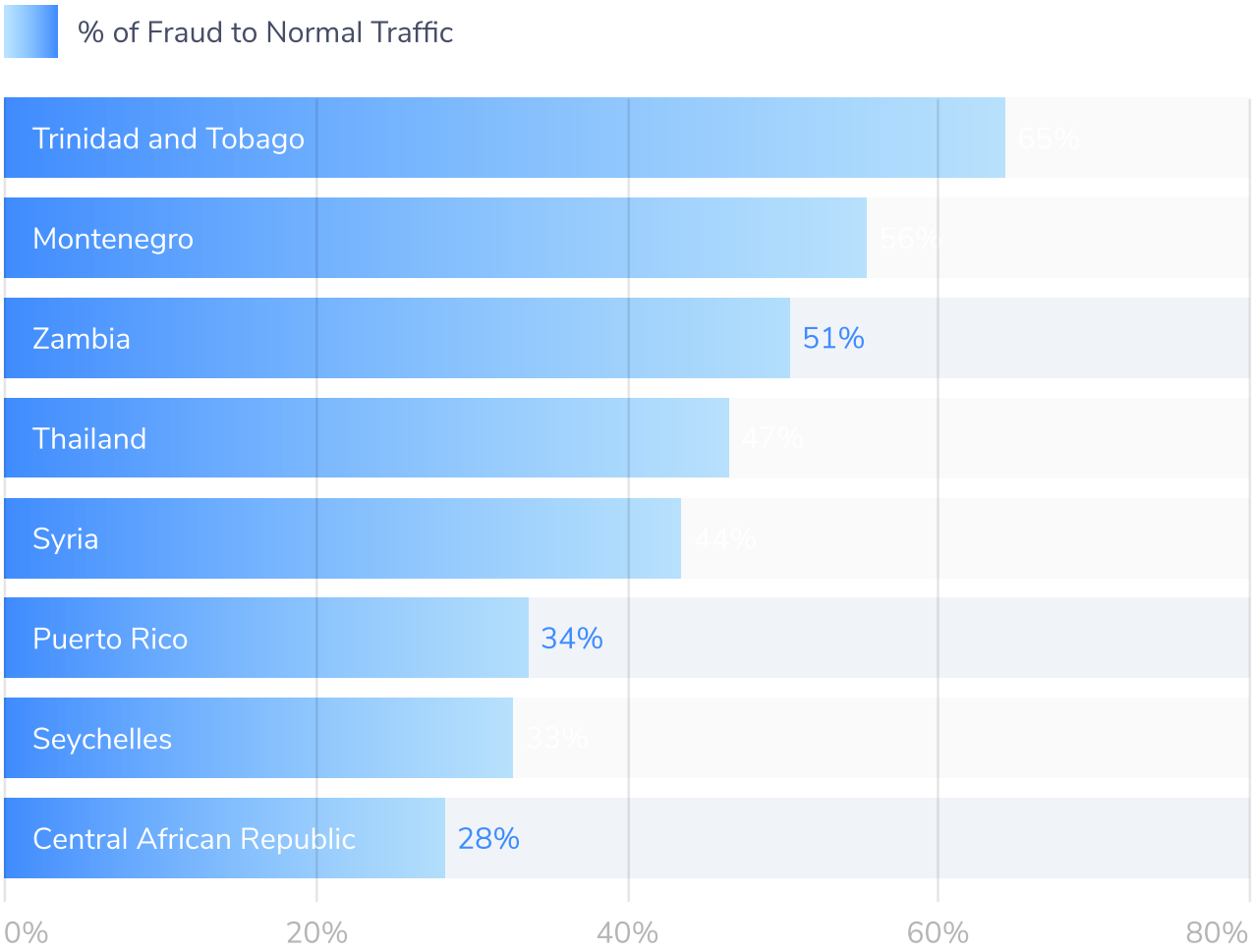
SPAM AND SCAM CALLS

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.

This section ranks the top 8 country range codes where flash call traffic originated, based on total call attempts during the quarter.

TOP FRAUD DESTINATIONS - % FRAUD TRAFFIC



SPAM AND SCAM CALLS

WHAT THE DATA TELLS US

This view highlights an important distinction between fraud volume and fraud prevalence. While the absolute number of spam and scam calls is important, the proportion of traffic identified as fraudulent provides another perspective on the scale of the problem within each destination.

The prevalence we see in the numbers is particularly interesting because spam and scam calls are ultimately consumer-targeting mechanisms. The traffic itself is only one part of the wider fraud chain: the greater concern is what happens when an innocent subscriber answers, engages with, or acts on a fraudulent communication. The telecom network can therefore provide an important signal of the attempted activity, but the eventual financial impact may occur elsewhere in the ecosystem, depending on whether a subscriber is successfully persuaded to disclose information, transfer money, or take another action.

This makes spam and scam calls strong examples of why telecom fraud cannot always be viewed in isolation. Telecom operators may see the attempted communication and its characteristics, while financial institutions may see the subsequent transaction or financial behavior. Neither necessarily has the complete picture on its own. Working across ecosystems can therefore provide a much stronger understanding of the complete fraud journey, from the initial communication through to any eventual financial impact.

The broader lesson is that a fraudulent call does not necessarily represent the end of the attack, but often the beginning of the customer harm. The communication may be used to establish trust, manipulate the recipient, or prompt an action that takes place outside the telecom network entirely. This means that understanding the legitimacy of the communication itself can become a valuable preventative control, helping organizations intervene earlier in the fraud journey rather than relying solely on detecting the financial consequences after the customer has already engaged.

For financial institutions in particular, extending visibility into the telecom layer can provide an additional opportunity to validate and verify the communications reaching their customers. Understanding whether a call is genuine, where it originated, and which numbers are involved in the communication can help establish greater confidence in the traffic before a customer acts on it.

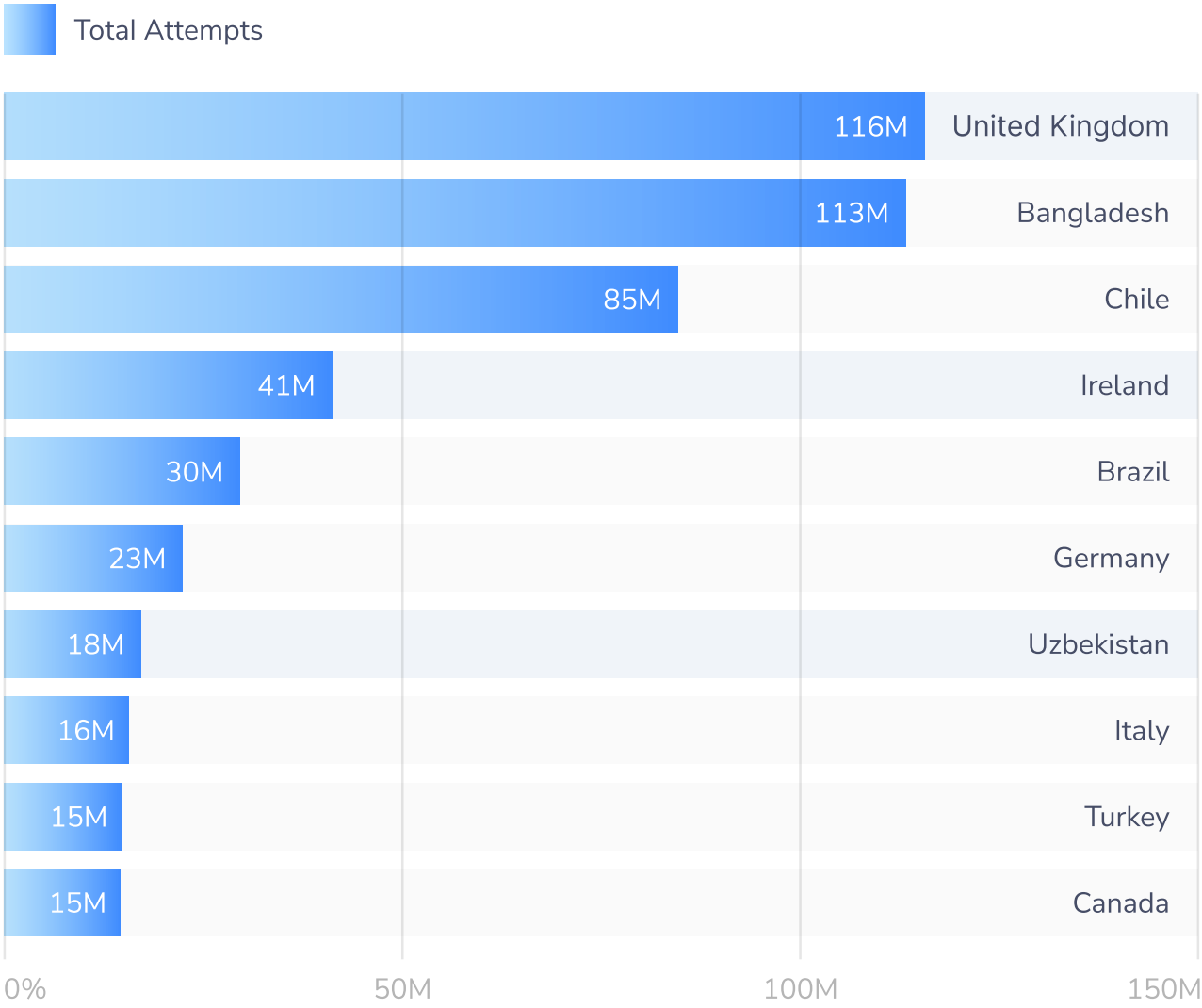
This is where AB Handshake's Call Validation technology can provide an important additional layer. Rather than simply identifying a call as suspicious based on its volume or destination, Call Validation is designed to certify and validate the A- and B-number of a call, establishing the calling and called parties and validating the legitimacy of the traffic. For financial institutions and other organizations exposed to social engineering fraud, this creates an opportunity to bring telecom intelligence into the wider fraud-prevention process and help protect customers from fraudulent calls made by actors impersonating legitimate enterprises.

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.

TOP TERMINATION COUNTRIES BY VOLUME



FLASH CALLS

WHAT THE DATA TELLS US

Flash Calls have become a high-volume global verification mechanism, rather than a niche alternative to SMS authentication. The UK recorded 116M attempts, closely followed by Bangladesh at 113M, with Chile reaching 85M. Further down the list, Ireland recorded 41M and Brazil 30M attempts, showing the enormous scale at which Flash Call verification can operate across different markets.

The volume also highlights why Flash Calls require a different approach to traffic analysis. Flash Calls are verification calls rather than conventional voice conversations, so very large numbers of short or zero-duration calls can be generated as part of legitimate authentication activity. Understanding this distinction is important when assessing whether unusually high traffic represents normal Flash Call usage or potentially abusive activity.

The scale of Flash Call activity also means that volume alone can be a relatively weak indicator of risk. As verification traffic grows, operators need to distinguish between expected high-volume behavior and activity that represents a meaningful deviation from normal usage. Establishing typical patterns by service, route, and market can therefore provide a stronger basis for identifying activity that warrants investigation than applying broad thresholds to call volumes alone.

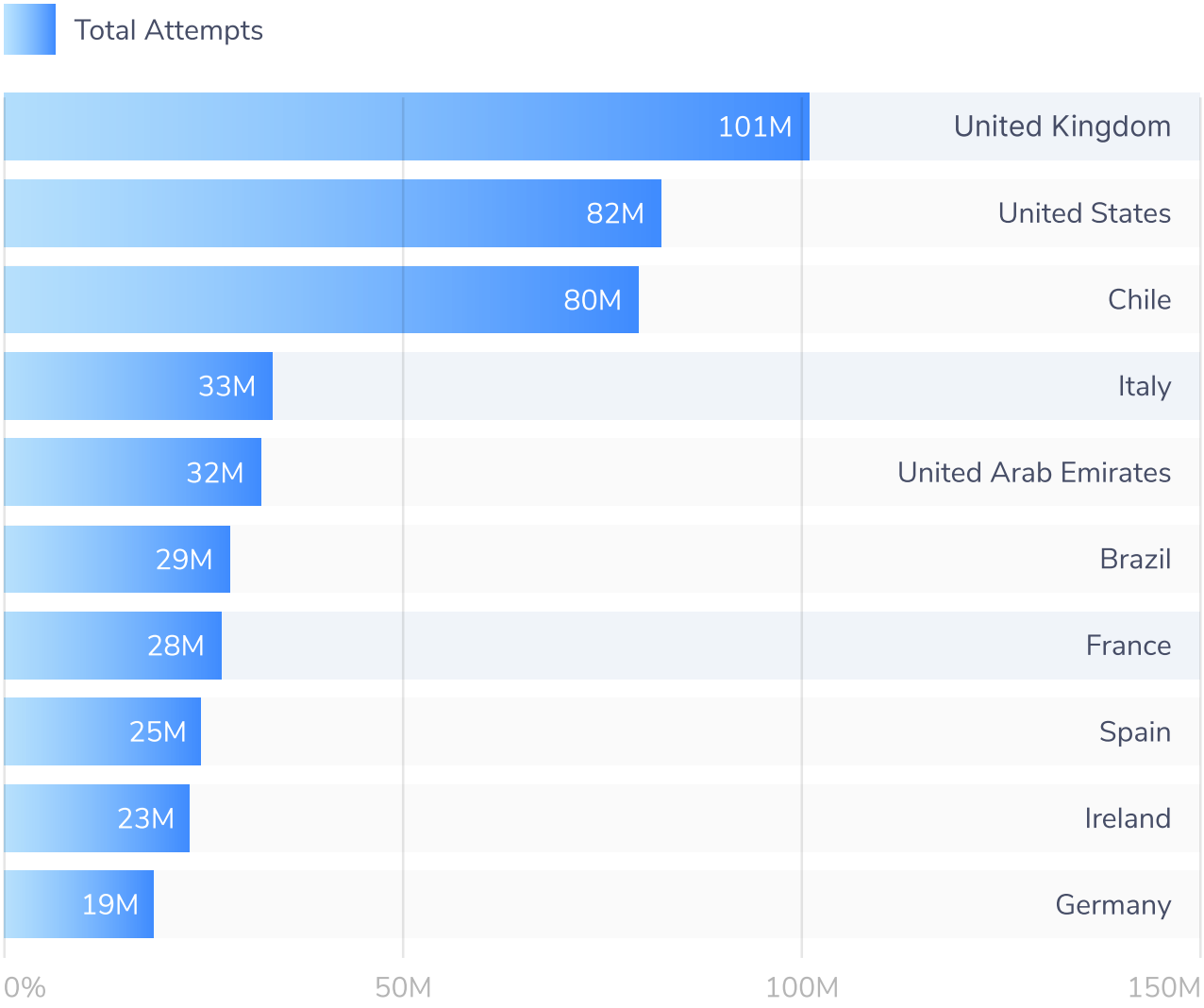
This is where AB Handshake's AI Shield can help operators make sense of high-volume traffic, using AI-driven analysis to understand traffic behavior in context and distinguish unusual or anomalous activity from normal Flash Call patterns.

FLASH CALLS

TOP 10 ORIGINATING 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.

TOP ORIGINATING COUNTRIES BY VOLUME



FLASH CALLS

WHAT THE DATA TELLS US

Looking only at termination countries tells us where Flash Call verification calls are being received; the originating view shows where the underlying Flash Call activity is being generated. Together, the two perspectives provide a much richer picture of the Flash Call ecosystem and how this traffic moves between markets.

The originating data shows the UK leading with 101M attempts, followed by the USA at 82M and Chile at 80M. Italy and the UAE follow at 33M and 32M respectively, with Brazil, France, Spain, Ireland, and Germany also appearing among the leading origins.

This distinction is particularly useful because high volumes in a termination market do not necessarily tell us where that activity originates. Looking at both sides allows operators to understand the relationship between source and destination, establish what normal Flash Call traffic looks like across different routes, and identify patterns that may warrant further investigation.

This broader visibility is another advantage of AB Handshake's AI Shield, which can analyze traffic across different points in the call journey and use AI-driven intelligence to identify unusual patterns that may not be apparent when looking at originating or terminating activity in isolation

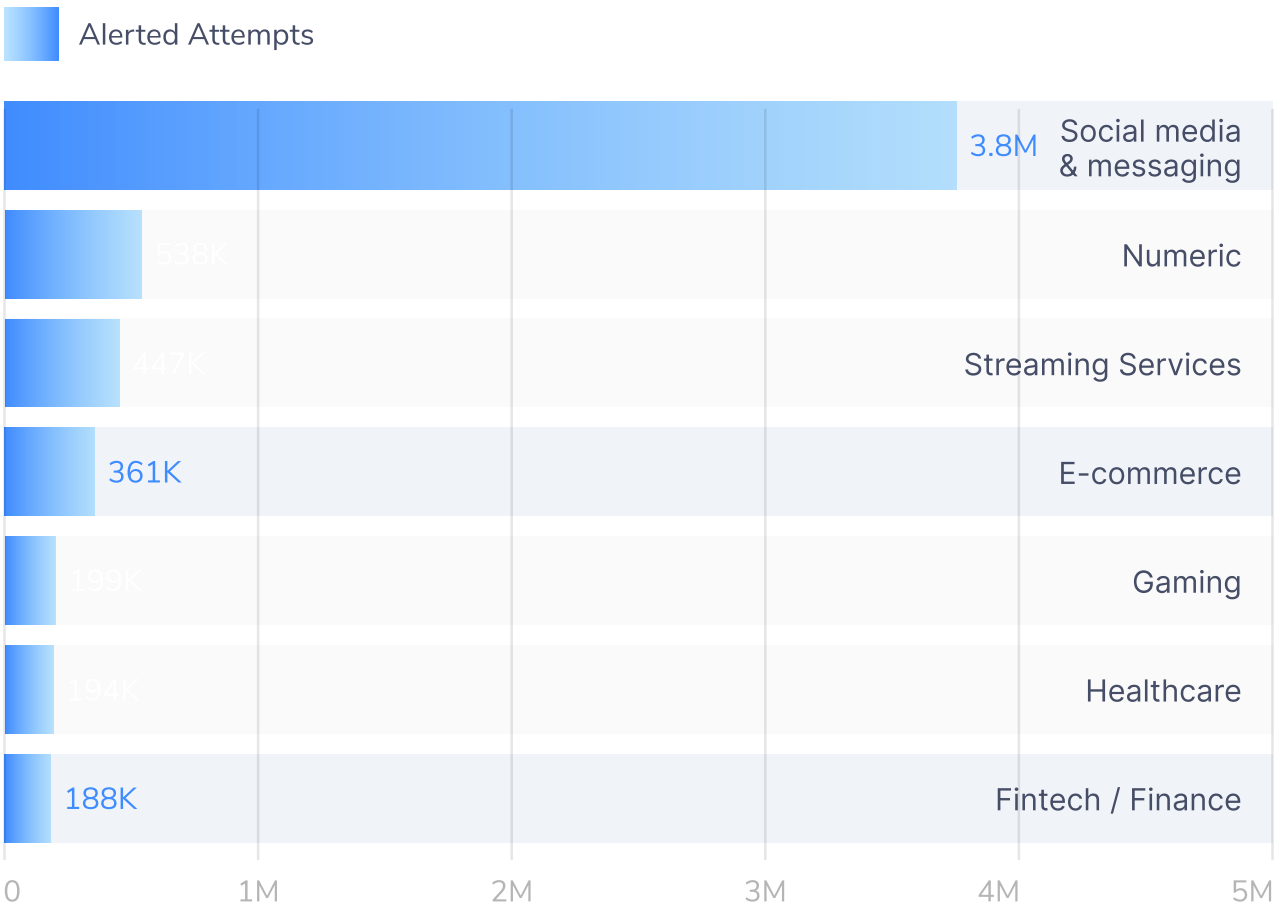
SMS AIT

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.

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

WHAT THE DATA TELLS US

SMS AIT activity is concentrated among a relatively small group of brands in the Q2 data. Telegram recorded 2M alerted attempts, followed by WhatsApp at 1M and Facebook at 576K.

The remaining entries in the top ten were a ‘numeric’ category (538K), Max (447K), Wilderberries (361K), TikTok (203K), NCSOFT (199K), Invito (194K), and Wise (188K). This gives a view of the brands most affected by alerted SMS AIT attempts during the period, spanning major messaging and social platforms as well as other digital services.

The data therefore shows that SMS AIT activity affected a range of different brands and services, with the highest volumes concentrated among Telegram, WhatsApp, and Facebook. Another important consideration is that AIT risk is not determined solely by the volume of messages being generated, but by the relationship between traffic and the legitimate demand behind it. A sudden increase in verification requests may reflect genuine customer activity, but it may also indicate that automated systems are being used to trigger messages without a corresponding legitimate user need. Understanding this context can help distinguish normal growth from traffic generated through systematic abuse of messaging workflows.

This is where AB Handshake can provide continuous visibility into SMS AIT activity, helping operators identify and monitor abnormal traffic patterns associated with different brands and services and helping protect revenue.

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