REDUCING MOBILE MESSAGING SCAMS

EVIDENCE AND OPTIONS FOR ADDRESSING CONSUMER HARM

Ofcom
OCTOBER 2024

BETTER MESSAGING
campaign registry

Introduction

In today's interconnected world, messaging campaigns have evolved into essential tools for businesses and organizations to engage effectively with their target audiences. However, ensuring the integrity, reliability, and compliance of these campaigns across a diverse set of platforms and carriers remains a significant challenge. The Campaign Registry (TCR), a pioneering information hub since its inception, addresses these complexities by both streamlining the registration process for messaging campaigns/ brands and by upholding industry standards.

TCR serves as a centralized platform dedicated to registering Application-to-Person (A2P) messaging campaigns. Its mission remains steadfast: to provide a simplified, fair, secure, and unbiased service by establishing common standards for messaging. Our solution offers a sanctioned A2P text messaging ecosystem that emphasizes transparency and reliability, benefiting both service providers and end users.

In this introduction, we've highlighted the pivotal role of TCR within global networks, as well as its dedication to shaping the future of messaging campaign management.

Background

TCR is an A2P messaging registry in the United States currently expanding our global reach. Our platform has been adopted by 1400+ aggregators, 4+ million global brands, and MNOs that cover 99% of US mobile subscribers. TCR registers the details around business messaging and associated senders who wish to send messages to other businesses and consumers in the US. Our solution currently supports more than 5 billion messages sent monthly over the 10DLC messaging channel. However, TCR is not an aggregator, gateway, or firewall — we only provide data and service portals to support MNOs and ecosystem participants in order to protect subscribers.

TCR has been witness to scams and fraudulent behavior in many countries and was created as a response to the current challenges being faced by brands, customers, regulators, and MNOs alike. Our solution helps prevent issues such as brand impersonation, CLI manipulation, spoofing, artificially inflated traffic, spam, and fraudulent promotions.

Some of our preventative measures include:

- Business verification of aggregators and brands as legitimate companies.
- Two-Factor Authentication (2FA) to prevent brand impersonation.
- KYC/KYB checks on businesses through a vetting process.
- Collection of legitimate Sender IDs.
- Blacklisting of exposed numbers.
- Verification of brands and campaign attributes.
- Real-time reporting of misuse and fraudulent activities.
- Reporting on the behavior of an aggregator's SMS traffic.

We've started to engage MNOs globally about rolling out a similar solution worldwide. We're aware of the current registry in the UK, and we feel that TCR can help expedite the onboarding of all participants in the SMS and RCS messaging chains, enhance communications, and mitigate fraud at the national level inclusive of all industry brands and merchants.

We welcome the opportunity to respond to your Call for Input: Reducing Mobile Messaging Scams.

Consultation response form

Please complete this form in full and return to mobilemessagingscamsresponses@ofcom.org.uk.

Consultation title	Call for input: Reducing mobile messaging scams
Full name	[redacted]
Contact phone number	[redacted]
Representing (delete as appropriate)	Organisation
Organisation name	The Campaign Registry
Email address	[redacted]

Confidentiality

We ask for your contact details along with your response so that we can engage with you on this consultation. For further information about how Ofcom handles your personal information and your corresponding rights, see Ofcom's General Privacy Statement.

Your details: We will keep your contact number and email address confidential. Is there anything else you want to keep confidential? Delete as appropriate.	Nothing [redacted]
Your response: Please indicate how much of your response you want to keep confidential. Delete as appropriate.	None [redacted]
For confidential responses, can Ofcom publish a reference to the contents of your response?	[redacted]

Your response

Question	Your response
Question 1: Do you agree that the routes described in this chapter cover all of the main methods that scammers use mobile messaging services to scam people? If not, please explain other methods.	Confidential? – N We agree that Ofcom covers the majority of known scamming methods in this chapter. We have, however, observed several other methodologies employed by bad actors in both the A2P and P2P messaging ecosystems:

Question	Your response
	• **Content spoofing/content injection:** When a scammer exploits a vulnerability in the messaging provider's APIs or routing gateway to intercept an insecure package and modify the message's content (usually a URL or Sender ID). The objective is to lure end users to a malicious website or to extract information. This usually occurs due to a lack of IPsec tunnels between gateway hops. • **Access hacking or credential hijacking:** When a scammer hacks a legitimate brand's account in a messaging provider's platform/API via wrongfully obtained or weak credentials acquired through brute-force methods. The scammer then uses this access to send their own malicious messages. • **Artificially Inflated Traffic (AIT):** Also known as SMS Pumping, this is a type of fraud attack where bad actors in the supply chain generate large numbers of SMS traffic for their own benefit. This is typically achieved by exploiting a lack of process controls on a brand's website or via their mobile application to trigger account creations or password resets. • **Global title spoofing:** Also known as GT Faking, this is another type of fraud attack where a bad actor changes a Mobile Application Part (MAP) parameter to manipulate information about the message's originator. This can be used to prevent detection by an MNO firewall and to impersonate a different MNO. **How does TCR address these scam methods?** Based on our experience, cooperation (on a national level) among regulatory authorities, MNOs, aggregators, a mandatory registry, and other parties is a crucial step towards preventing smishing, fraud, spam, and unsolicited messages. TCR's tested and proven approach has been instrumental in ensuring legitimate and safe A2P SMS messaging to end users. The following elements found in our own solution are of particular importance: • Mandatory brand and campaign registration ensures a single standard in the country for every business. This instills confidence that not just any organization can obtain Sender IDs without meticulous verification by a government-authorized body. • Encapsulating the key attributes of an SMS campaign such as brand name, Sender ID, sender number, use case, industry, MNO name, and aggregator name into a unique identifier (Campaign ID). This lets us share these data points

Question	Your response
	with relevant parties based on their role in the messaging ecosystem. • Comprehensive discrepancy analysis with options to suspend/block Sender IDs, campaigns, brands, and Tax IDs. This granular approach lets us tailor our solution to a country's specific needs. • Collecting and analyzing brand and campaign performance through real-time feedback on compliance from the firewall or SMSC. This allows us to share this data with other MNOs and relevant parties to potentially expose bad actors. • Offering a holistic approach to the messaging ecosystem where there's a clear separation of A2P and P2P traffic. This makes monitoring, investigating, and blocking potentially fraudulent traffic much easier. We encourage MNOs to frequently review P2P and A2P traffic in order to uncover any irregularities. MNOs can use these findings to make updates to their firewall policies to block leased GTs that are being abused.
Question 2: Which routes do you think are the most important today and will be over the next 3 years for the perpetration of mobile messaging scams? Please provide evidence for your views.	Confidential? – N We believe that today's most prevalent forms of mobile messaging scams are the following (and will continue to be important in the next 3 years): • Brand Impersonation • Brand Representative Impersonation • Smishing • Content Drift • Phishing In the future, these scams will largely proliferate in RCS and OTT channels. AI-driven methods are likely to grow, making messages and media content look incredibly plausible and better tailored to potential victims. Unfortunately, we cannot provide analytical evidence for trends as the data we hold falls under strict legal and operational regulations.
Question 3: Do you have any evidence specifically on what tactics scammers are using to access RCS messaging?	Confidential? – N In 2022, Google disabled RCS business messaging in India due to a surge in spam submissions. Based on our own assessment, this occurred due to the absence of robust spam controls and sender verification processes. As RCS continues to grow in market share across the globe, we anticipate that bad actors will devise new methods to bypass current anti-spam measures. They might exploit emerging technologies

Question	Your response
	(such as AI) to spoof and impersonate brand assets or push inappropriate content through RCS agents. Since RCS messages are encrypted and do not pass through firewalls, operators lack the ability to scan and block harmful content effectively. To mitigate these risks, we strongly recommend implementing a process of brand/sender identity verification to ensure that the sender is a legitimate entity and not an impostor. Additionally, an agent verification process should be in place along with periodic re-verification after the agent is live. This serves to validate the information inside the agent and ensures it is representing the brand correctly. These processes need to be the same for all MNOs within a country to facilitate accountability, compliance, and the ability to trace a message back to a legitimate entity.
Question 4: Are you aware of other relevant data sources on the scale or nature of scam messages sent over SMS and RCS?	Confidential? – N Publicly available sources and reports on the scale and nature of SMS scam messages should be scrutinized carefully. Many companies behind these free sources are usually selling products related to the ecosystem and are, therefore, in a direct conflict of interest. We've found that the most accurate data sources come from the mobile carriers themselves via an analysis of their overall P2P and A2P traffic. Unfortunately, the current data we do hold is subject to strict regulations and we are not at liberty to share it with external parties. As for RCS, it's important to acknowledge that it is a nascent messaging channel. Therefore, there are no exhaustive reports related to spam/scam messages, nor an in-depth analysis related to them.
Question 5: What is your understanding of which channels are supporting the greatest harm (such as A2P or P2P SMS, or RCS)? Please provide any supporting evidence.	Confidential? – N • **A2P SMS** has historically been the most vulnerable traffic due to its widespread use and lack of strong security standards and verification of sources. This makes it the primary vector for scams like phishing, Sender ID spoofing, and premium rate fraud. • **P2P SMS** can also be exploited through tactics like SIM swapping, social engineering, malicious SIM farms, or through P2P routes that are not properly monitored. • As a relatively new communication channel, **RCS** lacks fully developed sender identity verification and fraud mitigation processes. This allows scammers to impersonate brands, send illicit content, and get user information by exploiting RCS' capability to deliver rich and interactive content. As the channel grows, it will be extremely important to establish a

Question	Your response
	robust sender identity verification process to protect it from bad actors.
Question 6: What do you think will happen to RCS availability and adoption in the next few years? Please provide supporting evidence and or reasons for your views.	Confidential? – N With Apple's latest release of iOS 18, RCS' reach has expanded significantly. Coupling this with a high demand from brands to drive customer engagement using RCS' feature set means that many MNOs and aggregators are actively investigating support. It's no wonder then that industry reports forecast that the total RCS user base will surpass 2 billion by 2028. Wider adoption means that RCS will become more appealing to bad actors in the ecosystem. It is therefore extremely important to have a comprehensive sender and agent identity verification process in place. This will help identify who is sending what across the RCS ecosystem and ensure traceability and accountability. Based on our experience in the 10DLC SMS ecosystem, capturing the entire messaging chain is highly effective in identifying and eliminating any bad actors that might exist. Additionally, sender and agent identity verification is a necessary component in automating and securing the onboarding process in order to drive adoption and increase channel satisfaction. Based on comments from industry sources, many brands acknowledge that despite the success of RCS (over SMS) in their campaigns, the current manual onboarding process presents a significant obstacle. Different requirements and procedures across operators and aggregators are time-consuming and are impacting adoption. Unless these processes are streamlined, the channel will suffer. Brands often choose to prioritize this over pricing and other metrics when making decisions on how to engage with customers for their campaigns. TCR's RCS solution will help address these challenges and enable brands to quickly and efficiently adopt this new messaging technology.
Question 7: Do you have views on the effectiveness of the measures discussed in this chapter? For measures where we have identified specific issues, please comment on these in your answer, providing reasoning and evidence if possible.	Confidential? – N The measures outlined in the Ofcom chapter are quite good, but they won't fully address the industry's challenges without a holistic approach. Individual actions such as Sender ID policies, in-transit traffic blocking, and intelligence sharing will remain fragmented and will only be partially effective without a unified framework that ties all of the pieces together.

Question	Your response
	We recommend a mandatory, centralized registry that integrates the key components into a single solution, connecting all stakeholders across the UK A2P ecosystem via APIs and web portals. The essential components of this centralized registry would include: • Registry onboarding and verification of businesses (brands). • Brand vetting through online KYC/KYB checks in order to obtain access to specific use cases or verticals. • Assignment of a Sender ID to the verified brand and registering their A2P messaging. • Brand declaration of their registered messaging (with a description/sample). The registry would link it with the Sender ID and every participant name in the messaging chain. • Incorporation of the registry in MNO/firewall infrastructure via dedicated web portals and APIs. • MNO/firewall detection of registered and non-registered traffic by querying the registry's database in real-time. • Detection of malicious behavior performed by brands or aggregators reported to the registry in order to suspend A2P messaging traffic. This allows the MNO to make decisions and take relevant actions based on local regulations. For instance, in the UK, they could block the offending number, blacklist the violator, or apply fines amongst others if/as desired.
Question 8: Are there other measures that we should include in our assessment of the measures that can address mobile messaging scams?	Confidential? – N In addition to already taking steps to protect end users in the UK, we would strongly recommend incentivizing aggregators to register all traffic via an MNO-approved registry. Introducing mandatory registration to fully capture messaging content attestation, verified brand information, and all actors in the messaging chain will give MNOs the visibility and transparency that is necessary to investigate and mitigate messaging scams. It also provides them with a clear distinction between registered and unregistered traffic so that the MNO can decide whether to apply different policies depending on traffic classification. A registry can also provide tools for MNOs to set messaging limits and block traffic via brand, Sender IDs, or individual SMS/RCS campaigns as needed. It will also provide the traceability and evidence that will be required if/when fraud takes place.
Question 9: Within the options set out, what should be the priority areas, if any, to further disrupt mobile messaging scams?	Confidential? – N It is our opinion that targeting individual areas without a centralized, all-encompassing solution will not yield the desired outcome. The battle against mobile messaging scams must start by unifying the

Question	Your response
	different anti-scam methods via mandatory campaign registration. Without it, these efforts will remain fragmented and less than effective, as is currently the case. The major benefit of campaign registration is full visibility and traceability through all participants in the messaging chain. This includes brands, Tier 1, and Tier 2 aggregators. Registering Sender IDs alone is insufficient unless it can be tied to critical message attributes. Our framework encapsulates all key SMS and RCS attributes such as brand name, use case, specific industry vertical, unique Sender ID, MNO name, and aggregator identity into a unique identifier that can be queried by an MNO or its firewall vendor in real-time. This provides a clear distinction between valid registered traffic versus so-called "gray" traffic, enabling MNOs to act quickly and with confidence against potentially fraudulent activity. Armed with this information, MNOs can take appropriate action by suspending the messaging campaign, suspending the brand, or filing a complaint against the aggregator. Additionally, incidents reported by one MNO can be shared to all other MNOs in the registry ecosystem through automated, real-time event notifications, allowing all partners to be aware of suspicious or malicious traffic if this is desired (customizable based on local regulations and MNO needs). MNOs can further monitor the overall health of the messaging ecosystem through an embedded feedback loop. Reports can be generated on brands, aggregators, Sender IDs, and campaign IDs, highlighting instances of volume or content violations over a defined period of time.

Response to Additional Questions

Volume limits

Ofcom question:

5.9 - We believe consideration should be given to whether and how volume limits could be made more effective as a tool for disrupting scammers, without disrupting legitimate use. We would welcome views on how this could be done and the issues involved, including on:

- **How limits should be set and what constitutes a reasonable need;**
- **Whether limits should be standardized;**
- **What action should be taken if limits are breached; and**
- **What monitoring of limits should take place.**

TCR response:

RCS

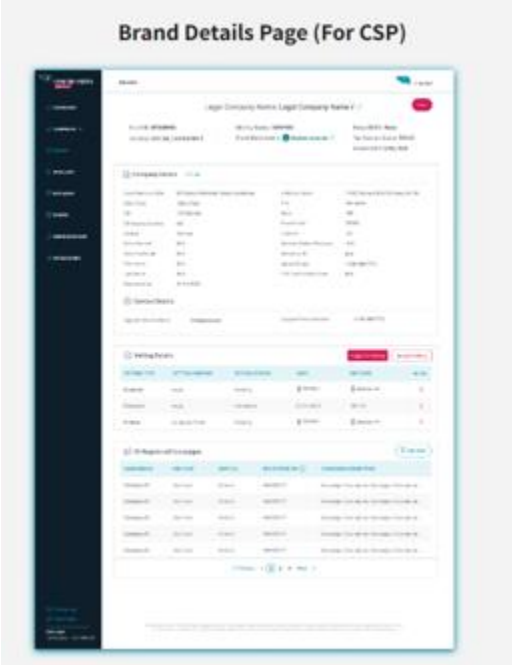
In order to stop bad actors from operating within the RCS ecosystem, there should be mechanisms in place to restrict or reduce messaging limits when an RCS agent exhibits non-compliant behavior.

This can be accomplished with a centralized RCS registry for brands and their RCS agents. Before messaging even starts, all brands would have their identities checked and their RCS agents verified. Then, RCS solution providers (such as Google) would actively monitor message compliance and share this data with the RCS registry (along with any spam and fraud reports).

An RCS registry could correlate this data with the associated brand and notify participating MNOs of any violations. With access to historical data available for brand/agent performance, MNOs could choose to reduce the message limit when necessary. RCS solution providers would be responsible for enforcing these limits based on the MNO's directives.

SMS

For A2P SMS messaging, TCR enables MNOs to establish individualized limits for each message use case (e.g., 2FA, marketing, political). These limits are visible throughout the ecosystem for all aggregators to follow and are enforced by MNOs. Additionally, MNOs can suspend campaigns or brands who repeatedly violate traffic limits via a web portal or API.



SIM registration requirements

Ofcom question:

5.13 - We would welcome views on whether SIM registration requirements merit any further exploration in the UK.

TCR response:

Many countries have implemented a proof of identity procedure for prepaid SIM and eSIM cards in an attempt to suppress fraud. As a standalone measure it has succeeded in making it harder for scammers to get a hold of large numbers of SIM cards. However, it has not significantly reduced other associated types of fraud unless additional measures were also adopted.

Suspension based on International Mobile Station Equipment Identity

Ofcom question:

5.17 - We would be interested in respondents' views on whether a similar approach to IMEI suspension could be effective in the UK.

TCR response:

We believe that IMEI suspension can be an effective measure to raise the cost of scamming attempts when it is simultaneously used to block an IMSI related to the IMEI. This renders a scammer's SIM cards and devices useless for illegal termination.

However, we feel that it's necessary to stress that any individual action will likely not suffice. This is why we strongly suggest taking a holistic approach toward addressing fraud-related issues in the messaging ecosystem. Combining multiple solutions in a coordinated fashion will result in the most successful outcome.

Our approach to this problem (with many fragmented parts) allows TCR to serve as a central hub for all stakeholders in the messaging ecosystem. Our registry links service providers, brands, firewall providers, MNOs, direct connectivity aggregators, and regulatory authorities together to enable greater transparency and raise the overall trust in a message's origins and content. It is only through clear collaboration between the aforementioned parties that we can assure the integrity and security of the messaging ecosystem.

Intelligence sharing and reporting incentives

Ofcom question:

5.32 - We would welcome input from stakeholders on how else intelligence is shared amongst aggregators and operators and any ways in which this could be improved.

TCR response:

The current challenge with intelligence sharing in the industry is that it typically occurs in a reactive, post-fact manner. A more proactive approach would be to provide real-time suspension alerts to all MNOs and aggregators involved in a messaging campaign.

TCR's current messaging solution allows MNOs to quickly suspend problematic messaging campaigns or brands via a web portal or API. These suspension alerts include a category and description related to the violation, providing more context for proper remediation. Whenever a messaging campaign or brand is

suspended, Tier 1 and Tier 2 aggregators are immediately notified through suspension events, which they then honor by stopping traffic.

Challenges surrounding A2P messages and questions for stakeholders

Ofcom question:

5.34 - We would welcome views from respondents on what more can be done to make the A2P route more impervious to scams. In particular we are interested to understand views on:

- **What could be done to further drive good practices amongst the aggregator sector;**
- **Whether more standardization would help to close the loopholes that scammers have sought to exploit;**
- **How effective KYC checks are across the aggregator supply chain, especially where there are many parties involved in the delivery of messages; and**
- **How best to mitigate associated supply chain uncertainties, such as by building on the contractual obligations and dedicated connections described above, taking steps to reduce the number of parties in the supply chain, or other methods.**

TCR response:

• ***What could be done to further drive good practices amongst the aggregator sector?***

Mandatory registration of all A2P messaging traffic within the country would encourage all aggregators to adhere to best practices. Tier 1 aggregators should be required to review each registered messaging campaign for compliance before granting approval for provisioning. Full visibility of all participants in the messaging chain would also foster a framework of accountability, ensuring that aggregators are fully responsible for the traffic they deliver to MNO networks.

• ***How effective KYC checks are across the aggregator supply chain, especially where there are many parties involved in the delivery of messages?***

In our experience, we've found that current KYC checks are not standardized among Tier 1 aggregators and that there are no third-party verification agencies involved. This makes it easier to abuse and impersonate those aggregators. With messaging registration, there's greater transparency between parties (where appropriate). This allows multiple KYC checks to be performed before sending traffic.

• ***How best to mitigate associated supply chain uncertainties, such as by building on the contractual obligations and dedicated connections described above, taking steps to reduce the number of parties in the supply chain, or other methods?***

Ensuring full transparency and visibility across MNOs and Tier 1 aggregators is the most effective way to mitigate uncertainties in the messaging supply chain. Regardless of the chain's complexity, each participant needs to be registered and linked to both the message content and the brand. Traceability can then be achieved, with each participant held accountable for their role, and their compliance monitored by MNOs.

Measures to address RCS scams

Ofcom question:

5.39 - Our understanding of these measures, and other steps that may be being taken to stop scams accessing RCS networks, is limited. Therefore, we are seeking input from stakeholders on the full range of measures that are used to protect consumers and their effectiveness.

TCR response:

As a new channel, RCS currently offers fewer options to protect consumers from scam/spam than SMS. As RCS continues to evolve, we suggest employing the following measures to help secure it:

- **Sender Identity Verification**: A thorough and all-encompassing brand identity verification process will be crucial to ensure that RCS A2P messages are sent from a verified sender. While RCS currently supports a verified sender checkmark, there aren't any effective standards for verification, making this channel vulnerable to scams. TCR recommends a single brand identity verification process across all MNOs within a country with standardized verification requirements.
- **Agent Verification**: Agent verification will be necessary to make sure brands are represented correctly and that the content in the message flow is appropriate to the use case.
- **Active Compliance:** An AI-based content filter on the RCS service provider can help ensure there is no content drift from what was registered. Deviations from registered content need to be reported back to a centralized registry and attributed to the brand.
- **Feedback Attribution**: End users currently have the ability to report if a message is fraud/spam. However, this feedback is not directly associated with the brand. Fraud and spam data needs to be connected to the brand in a centralized RCS registry to ensure that any bad actor is identified and appropriate action is taken.
- **Periodic Monitoring**: RCS agent content will need to be periodically verified to ensure that the content matches what was registered.

Limitations of traffic monitoring tools

Ofcom question:

5.48 - We are interested in exploring whether and how the use of these tools can be made more effective across industry. We would particularly welcome views from stakeholders on:

- **Should more parties, like MVNOs and aggregators, be making use of similar tools?**
- **How can existing tools and the human systems around them be better configured, or made more sophisticated?**
- **Would more consistent implementations across parties, and better-quality information sharing improve blocking efforts, and how might these be achieved?**

TCR response:

- ***Should more parties, like MVNOs and aggregators, be making use of similar tools?***

As far as we know, most Tier 1 aggregators and MVNOs have already implemented such tools (especially in the form of text pattern-based filters). However, scammers are always probing these tools in order to reverse engineer how they work and what they don't block, so their effectiveness is not absolute. For example, they might intentionally use grammatical errors or misspell famous brands in order to avoid these filters, or they might use different character encoding sets to avoid GSM7-based filtering.

- ***How can existing tools and the human systems around them be better configured, or made more sophisticated?***

These systems must be implemented properly and proper analysis must be used to be able to interpret the information. There have been multiple incidents in the past where these systems blocked legitimate traffic or were not functioning properly due to a bad configuration.

TCR's solution actually works with these existing systems to enhance them and make them foolproof when spotting fraud.

- ***Would more consistent implementations across parties, and better-quality information sharing improve blocking efforts, and how might these be achieved?***

Our web portal and API solutions can enable all MNOs within a country to share compliance breaches and suspension events for suspicious SMS campaigns. Suspensions can be done in bulk or by a single campaign and include a category and explanation visible to all parties in the messaging chain. This helps to provide clarity and important information to other MNOs in order to determine if they need to take action. Suspension and compliance data is also shared with other relevant parties in the messaging ecosystem based on their role and customized according to local regulations and MNO needs.

RCS and traffic monitoring tools

Ofcom question:

5.50 - We would welcome further input from stakeholders on what can be done, and on what is being done, to identify suspicious RCS messages in transit.

TCR response:

Unfortunately, the exact measures currently used by RCS service providers are not shared publicly. However, we recommend utilizing a combination of the following proactive and reactive strategies to help identify suspicious RCS messages in transit:

- **Content Filtering and Analysis**: Natural Language Processing (NLP) tools enabled at the RCS service provider can flag messages containing known spam, phishing phrases, suspicious URLs, or inappropriate language. Flagged messaging data can then be shared with the RCS registry and attributed back to the brand.
- **Behavioral Analysis**: Machine learning models can also be employed by RCS service providers to identify abnormal sending patterns or deviations from established baselines. This data can also be shared with the RCS registry and attributed back to the brand.
- **User Feedback (Report Spam/Fraud):** Users are able to report spam and fraud received from RCS agents. Sharing this data with a centralized RCS registry and attributing it back to the brand can help MNOs make a decision on whether to suspend the brand/agent.
- **Performance Analysis:** Using customer feedback data or content filtering/analysis models, an RCS registry can provide detailed performance data about agents back to MNOs. These analytics can then be used by different entities to identify bad traffic patterns and hold senders accountable.

Sender ID registries

Ofcom question:

5.62 - For the UK, we are interested in stakeholders' views on the best way forward. Broadly, there appear to be two main approaches:

- **Firstly, to continue with the registry run by the MEF and to seek to make it more effective (such as through wider adoption by brands that haven't yet signed up, or by moving closer to a real time approach); or**
- **Secondly, to switch to a mandatory approach as adopted by other countries described above, which would need to be run by an appropriate organization.**

TCR response:

Taking into consideration the available resources, timelines, and urgent industry needs, we strongly recommend switching to a mandatory registry operated by an independent party, as has been successfully adopted by other countries.

Based on our professional experience from working in other markets around the world, we firmly believe that a partial SMS registry isn't sufficient to tackle the UK's current challenges. While partial SMS registries have provided some support and improvement, they are not an industry solution. They're limited to a small number of brands within a greater pool of millions of brands who want to protect their A2P messaging.

These are a few of the challenges a country can expect when employing a partial registry solution:

- Only a small number of aggregators and operators in the given country take part in the initiative.
- There is no supporting technology to enforce it. The process is labor intensive and based solely on manual reporting either in a spreadsheet or online dashboard.
- There are typically no checks or audits to confirm that the participating aggregators are actually protecting Sender IDs/brands and blacklisting them. There is no verified database and it does not operate in real-time.
- The solution is limited, only available to a small number of brands/merchants within the country. End users continue to experience spam and smishing at ever increasing levels. When there are thousands of brands/merchants in the country, protecting only a few dozen does not have a substantial impact on fraudulent activity.
- Partial registries rely on the participants' own diligence and trust. When an issue occurs, it has to be reactively remediated, taking a significant amount of time and resources. Unfortunately, at that point, the damage is done. If a proactive solution had been implemented, it could have prevented the damage from ever occurring in the first place.
- Data privacy and management of the sensitive information is not automated, making it vulnerable to human error.
- Partial registries also tend to be cost prohibitive for the relevant parties. An industry solution should be affordable, easy to use, and easy to access for everyone.

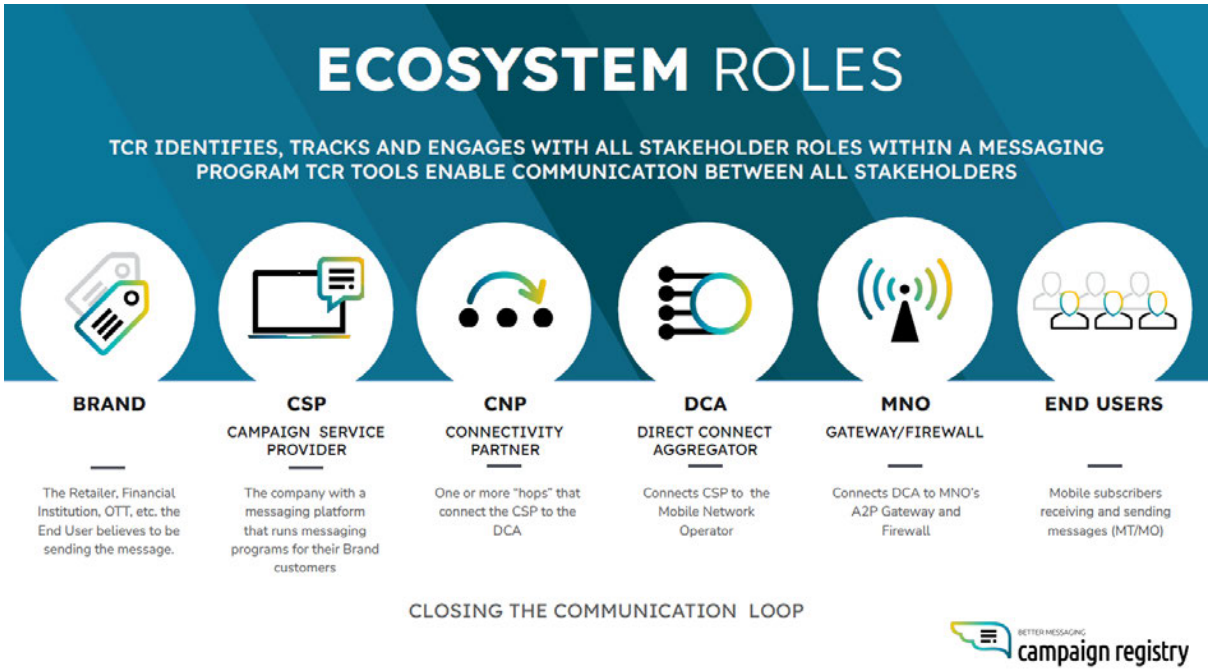
Based on these observations, our recommendation is to switch to a mandatory registry, as other countries have adopted. In order to maintain objectivity, this registry should be run, ideally, by an independent third party who is not in the path of the message, nor able to see the message's contents.

TCR's own registry is a proven solution that has been very successful in the United States and is currently expanding into other territories. In our first 12 months of operation, we onboarded more than 1,300 global aggregators, registered and verified over 3 million global brands, completed integration with the four main

MNOs in the US, and launched over 3 million campaigns, supporting over 5 billion SMS messages every month.

We can also confirm that there are already 32 local British aggregators (on top of the global ones that also operate in the UK) and 3,022 local British brands already registered in TCR. We therefore anticipate a much quicker adoption and implementation when launched in the United Kingdom.

TCR has the necessary staff and experience to onboard all industry participants, from brands/businesses to aggregators and MNOs in a relatively short period of time.



In summary, we would recommend:

- **Centralized KYC/KYB methods embedded in a streamlined online process.** TCR is an independent party, and it's not in the path of the message. It is a proven solution currently providing a platform with web portals and APIs for each stakeholder in the messaging ecosystem. If required, we could provide Ofcom with its own dedicated portal for monitoring purposes.

- **An online platform that provides visibility to industry participants across the whole messaging chain.** TCR helps mitigate brand impersonation, smishing, and spam by providing a feedback loop for all parties. This information helps the ecosystem make informed decisions regarding campaigns, brands, and aggregators.

- **Establish a clear differentiation between A2P (Application-to-Person) and P2P (Person-to-Person) messaging.** A2P messaging can be defined as registered traffic traveling through a messaging registry where the necessary commercial and regulatory rules can be applied in a proactive manner (i.e., predefined by regulatory bodies and MNOs). This registered traffic would have these rules applied, leaving the rest of the traffic to fall under higher scrutiny P2P rules/guidelines.

- **Grant MNOs the ability to only allow preregistered brands and campaigns to send messages on their network.** A mandatory registry such as TCR's can enable MNOs to prevent message transmission before a brand's identity verification and Sender ID registration is complete.

- **Allow MNOs to establish different tier-based restrictions based on a brand's identity status.** For example, brands who opt for basic verification get a lower throughput of messages, whereas brands with enhanced verification get a higher throughput.

- **Let an independent entity that is not part of the ecosystem's messaging flow manage this solution.** This provides an objective messaging registry and authority who can ensure a fair ecosystem.

A project like this requires close coordination and cooperation between the relevant parties in the country's ecosystem, primarily the messaging platforms (who represent their brands), the vetting providers, the gateway/compliance providers, and MNOs. We can facilitate establishing this cooperation, as we have prior experience in this area.

TCR currently acts as the sole registry for 10DLC A2P messaging in the US, mandated by all of the country's telecom operators. TCR can replicate this model for the United Kingdom, ensuring that the latest technology and international standards are implemented to combat fraud. Currently, TCR has active, biweekly working group meetings with MNOs, aggregators, and an antitrust partner in the US. A similar approach could be adopted in the UK with Ofcom as a participant, if desired.

In order to provide more insight into how different types of spam and fraudulent activity are addressed by mandatory vs voluntary registries, we present the following table:

Problem	Solution	Mandatory TCR Registry	Voluntary Sender ID Registry
Fraudulent aggregators/AIT	A connectivity partner visibility tool MNO-defined and monitored message limits per partner, brand, and use case	Yes	Limited
Content drift/injection	MNO/firewall message checking against content samples stored in the registry	Yes	No
Spoofed Sender ID	A Sender ID online database integrated with MNOs/firewalls, linking critical messaging attributes with Sender IDs	Yes	No
Messaging spam	Message limit filters at the firewall that can report violations to the registry and MNOs Message content registration and in-transit checking at the firewall with discrepancies reported to the	Yes	No

	registry and/or MNO		
Brand impersonation	Packaging of Sender ID and messaging content with KYC/KYB checks via brand vetting	Yes	Limited
Message blocking	Blocking via discrepancy alerts in the registry with detailed explanations	Yes	No
Spam/fraud alerts	A feedback reporting and alert tool	Yes	No

MNO Sender ID policies

Ofcom question:

5.65 - We welcome views on the efficacy of these additional policies, and whether there would be benefits to ensuring similar measures are taken across MNOs in a standardized fashion.

TCR response:

The effectiveness of Ofcom's proposed measures relies on a standardized and integrated approach, as exemplified by TCR's own registry. A registry needs to be central to the messaging ecosystem, with MNOs endorsing and supporting its implementation nationwide.

A standardized Sender ID policy for SMS business messaging should be formalized and communicated to all parties in the ecosystem. Mandatory verification of brands and aggregators, overseen by an MNO-designated verification authority, should also be a part of the central registry. Registration of Sender IDs alone is insufficient; it must include critical attributes like a use case, sample message content, and brand details to ensure comprehensive and integrated oversight. Tier 1 aggregators must qualify and attest to messaging traffic in line with MNO policies, tailored to each brand and type of message. This process provides MNOs with the transparency needed to monitor who is delivering messages and what is being delivered.

The established framework also needs real-time monitoring tools and mechanisms so that MNOs can respond to violations. By integrating a registry with MNO and firewall infrastructures, firewalls gain access to critical data including registered messaging details and blacklisted Sender IDs. This allows them to detect content discrepancies, message limit violations, and any misuses of Sender IDs or use cases.

When equipped with this information, the MNO/firewall can make informed decisions on whether to suspend suspicious messages, while the registry's ability to trace a message across the connectivity chain reduces the likelihood of legitimate messages getting accidentally blocked.

With this setup, any time lag between the suspension of suspicious messages and their blocking is reduced, enabling MNOs to act swiftly. In TCR's own registry, MNOs can automate the suspension of traffic or brands via an API interface or manage this process manually through a web portal.

RCS verification

Ofcom question:

5.66 - As described at paragraph 5.37 above, business senders have to be registered with and verified by a verification authority. We would welcome insights from stakeholders on how well this process works currently.

TCR response:

In the current RCS model, either the RCS Service Provider (Google) or the MNO is responsible for the verification of RCS agents. This is dependent on the contractual relationship between the MNO and Google.

If MNOs are responsible, they must either a) complete the verification themselves, or b) work with a verification authority. This results in a disconnected verification framework where there are different processes for different MNOs. With each MNO capable of defining their own verification requirements, this leads to operational challenges, longer onboarding times, and higher costs for brands and aggregators. This approach is not scalable and provides loopholes for bad actors.

We recommend a single RCS registry that features the following elements:

- A single and unified onboarding process offering quick, easy, and cost-effective onboarding for all MNOs within a country.
- Unified verification requirements for all MNOs within a country.
- A network of MNO-designated verification authorities integrated with the RCS registry. These authorities would perform brand and RCS agent verification based on the unified verification requirements.
- One-time verification of brands and RCS agents for all participating MNOs in a country.
- An ability for MNOs to review the brand verification details and any associated A2P messaging compliance history. This would provide a final step of approval before the RCS agent is launched.

TCR's RCS solution offers all of the items above and is based on a proven SMS registry with over 3M+ registered and verified brands.

Ofcom question:

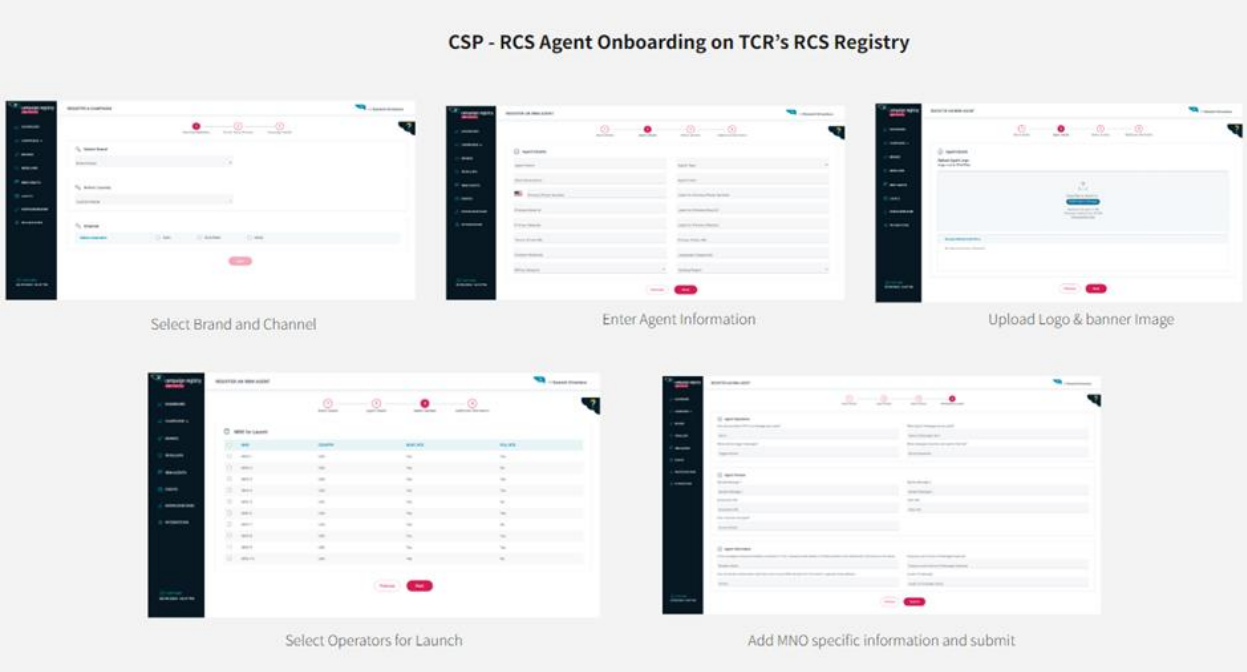
5.67 - We are not aware of other tools, such as Sender ID registries, designed to specifically protect brand IDs for RCS, but would welcome input from stakeholders if other mechanisms are used.

TCR response:

TCR has also been working on an RCS Registry solution.

Since RCS is a developing technology, there aren't many tools available to protect against brand impersonation. As described in the previous answer, we recommend having a unified registry solution such as TCR for both SMS and RCS. This way all A2P activities connected to a brand can be traced back, ensuring a higher level of compliance, visibility, and control.

This approach would also allow brands, aggregators, and MNOs to use the SMS channel as a fallback solution for RCS campaigns, if needed. TCR currently has 4M+ brands verified for SMS messaging. By collecting a few additional details, these brands can also be verified for RCS, offering a quick path to scale.



Education

Ofcom question:

5.74 - We would welcome suggestions of any other approaches which could be used to effectively support consumer education on mobile messaging scams.

TCR response:

We believe that the UK is currently doing well in this area. Industry experts (which include brands, aggregators, MNOs, regulatory bodies, and other associations) actively participate to improve collaboration and consumer education.

If given the opportunity to establish a registry, we would be an active member of the ecosystem, supporting MNOs and key stakeholders to increase consumer awareness and support industry initiatives. There is so much more that needs to be done to tackle fraud and minimize functional impact and financial losses. We can only accomplish this by working together.

Identifying or filtering suspicious messages on the handset

Ofcom question:

5.79 - We welcome input from stakeholders on any ways in which handset-based solutions could be improved or used further to help consumers.

TCR response:

We believe that the market already offers an adequate number of solutions for handset-based blocking and reporting through both native operating system applications (Android and iOS) and third-party applications. Our only further recommendation is to raise end user awareness on how and where to report scams. That

will be especially important for RCS as Google is the only entity who can see content and potentially block it.

Reporting suspicious messages

Ofcom question:

5.85 - We welcome input from stakeholders on how consumers could be better supported to report suspicious messages. For example, are there ways to make reporting tools more widely accessible to consumers, and could more be done to distinguish between suspected scam and spam messages (either through consumer facing services or through design of back end systems used for analysis)?

TCR response:

The UK already has public-facing methods of reporting spam, either by calling 0300 123 204, forwarding messages to a dedicated shortcode (7726), or by using the Action Fraud website. Similar to our previous suggestion, we recommend raising awareness among end users on how to recognize fraudulent and spam messages and where to report them.

Also, TCR provides a Feedback Loop that could be implemented to support tackling the current gaps in the above methods whilst also exploring new solutions to mitigate these ever evolving industry challenges.

Measures taken to disrupt mobile messaging scams: summary

Ofcom question:

5.87 - In terms of stopping scam SMS messages from entering mobile networks through P2P channels, we are particularly interested in stakeholder views on whether volume limits could be made more effective as a tool for disrupting scammers. For A2P, we are interested in what could be done to further ensure that due diligence is effective across the whole supply chain.

TCR response:

We've found that imposing volume limitations based on a unique Sender ID from the MNO side can be particularly effective, especially when combined with advanced data analytics that track volume trends within a specific time frame per brand or use case.

Most large international organizations have a predictable and steady volume of messaging traffic associated with their operations (e.g., social networks using A2P channels for two-factor authentications, or financial institutions notifying end users of payment actions). If major changes in traffic volume are detected, MNOs in TCR's registry can compare volumetric statistics against data points for a specific brand and their use cases. This helps the MNO determine if activities like SMS Trashing and Artificial Traffic Inflation are occurring. Without access to a registry that provides this information, these types of fraud would be difficult to detect.

Additionally, should the MNO determine that these fraudulent activities are happening, they can use our API or web portal to suspend those campaigns based on Sender ID, UTR (Tax ID), or the brand itself in order to prevent further damage. Our registry allows these suspension events to be shared with relevant

parties in the supply chain, shining a light on potential bad actors in the ecosystem.

Ofcom question:

5.88 - To identify suspicious SMS messages in transit, we are interested in what can be done to build on the existing success of MNO blocking processes, which could include through wider adoption (by more MVNOs or aggregators) or better application of existing tools. On A2P channels, we have set out a number of different design features of Sender ID registries and would welcome views on the best way forward in the UK context to build on existing measures.

TCR response:

When considering a Sender ID registry for A2P channels, our experience has shown us that the most important feature is to provide full visibility and traceability of a message across the entire messaging chain. Being able to trace a message's journey from brand to aggregator to MNO and finally to end users eliminates any opportunities for bad actors to evade detection.

Additionally, we believe that any established registry should be integrated with an MNO's firewall infrastructure. This would let MNOs receive alerts the moment suspicious traffic is detected, allowing them to take action to block or suspend messages. When there's a registry that provides information as to what a legitimate message should look like, its Sender ID, and the delivery path it should follow, MNOs are then armed with the necessary data to make informed decisions.

Ofcom question:

5.89 - Support for consumers to identify and report suspicious messages, such as through education and device-level services, is also important. We are seeking stakeholder views on how well existing measures in this area are supporting consumers and what more could be done.

TCR response:

As we've previously noted, the UK currently has an established process in place for reporting suspicious messages from end users (by calling 0300 123 204, forwarding messages to shortcode 7726, or by using the Action Fraud website). There also exists built-in operating system-based reporting within messaging applications. Our only other suggestion beyond a mandatory registry would be to conduct more public marketing campaigns in order to raise awareness among end users.

We strongly believe that establishing a mandatory registry will ultimately instill the greatest confidence for using messaging as a trusted business channel. End users would know that each brand is verified by third-party MNO and government-approved vetting agencies, and that there is a clear supply-chain trace (along with other data points) that can be used to identify bad actors.

Ofcom question:

5.90 - Protecting consumers from RCS scams requires different approaches in some areas, not least due to end-to-end encryption. Our understanding in this area is currently limited but we recognize that it may be a significant area of potential growth for future scam messaging activity. Therefore, we are seeking more information on what is done at each stage of measures set out in this chapter as well as any data on how effective these measures are.

TCR response:

Since RCS P2P messaging is encrypted end-to-end, it is difficult to monitor traffic or put active compliance measures in place. RCS A2P messaging is decrypted at the service provider level, meaning that messages

can be directly attributed to the sender/brand in a centralized registry. Sender verification and feedback is a highly effective approach and is currently used to secure the SMS A2P channel in the United States.

In Conclusion

The existing validation and verification of businesses through KYC/KYB methods is not sufficient if an A2P message is not tamper-proof through its entire journey from the originating source to the subscriber's phone.

In the British market, emphasis should be placed on implementing a technological solution for commercial traffic registry that can be promptly and efficiently adopted by the industry. It's crucial to identify an independent third-party entity to serve as the front of the registry and stay abreast of the constant challenges posed by fraud and spam. This entails employing experts and allocating resources for deployment, maintenance, and staying updated with emerging challenges through an efficient team of developers. Additionally, resources must be allocated swiftly to onboard all participants in the messaging chain, including brands, mobile network operators (MNOs), direct carrier aggregators (DCAs), communication service providers (CSPs), content network providers (CNPs), firewall providers, and regulators.

The Campaign Registry provides a cornerstone in fostering trust, reliability, and compliance within the A2P messaging landscape. By registering A2P campaigns, TCR enables transparency and accountability, facilitating MNOs in delivering a more reliable and predictable messaging service. Through collaboration with aggregators, brands, and other stakeholders, TCR contributes to establishing a sanctioned and accountable messaging environment, benefiting all participants in the A2P messaging chain. Implementing these measures, managed by TCR, will significantly contribute to mitigating fraud in the UK.

As a trusted partner of mobile operators, regulatory bodies, and aggregators in different countries, TCR looks forward to collaborating with Ofcom and industry stakeholders. Together, our messaging solution can help deploy cutting-edge KYC methods to address the existing challenges in the UK.

We have already been in conversations with the Big 4 Mobile Network Operators in the UK and other relevant industry bodies and associations (Google, MEF, GSMA, Home Office and UK Finance) and we demonstrated our platform and its capabilities for both SMS and RBM messaging. We would like to extend an invitation to meet with Ofcom and relevant participants to also provide this demonstration, hear your feedback and further needs, and provide a trial of our solution.

We thank you for the opportunity to address your call for input and for taking the time to read our response.

Best regards,

The Campaign Registry team.

Glossary

API - Application Programming Interface. A type of software interface that allows different applications to communicate with each other.
A2P Messaging - Application-to-Person messaging is a type of message traffic sent from a business to a mobile user, usually via an automated process, typically related to marketing or professional service activities.
Brand - The company or entity the end customer believes is sending the message.
Campaign - Attributes of a message that will reach an end user.
CNP - Connection Network Provider (e.g., aggregator, CPaaS company, messaging provider).
CSP - Campaign Service Provider (e.g., Tier 2 aggregator, CPaaS company, messaging provider).
DCA - Direct Connect Aggregator (e.g., Tier 1 aggregator, CPaaS company, messaging provider).
FW - Firewall.
GT - Global Title. An address used in the SCCP protocol for routing signaling messages across various telecommunications networks.
GW - Gateway.
KYB - Know Your Business. A process used by various industries to establish a business' identity and authenticity.
KYC - Know Your Customer. A process used by various industries to identify and verify a customer's identity.
LC - Long Code (10-digit number).
MNO - Mobile Network Operator.
Phishing or Smishing - An attack technique that tricks mobile network subscribers into sharing their personal or sensitive information (such as credit card details).
RBM - Rich Business Messaging - RCS for Companies (A2P RCS).
RCS - Rich Communication Services. A newer communication protocol that offers a more enhanced messaging experience compared to traditional SMS messaging.
SC - Short Code.
SCCP - Signaling Connection Control Part. A network layer protocol that provides extended routing, flow control, segmentation, and error correction facilities in telecommunications networks.
SIM - Subscriber Identity Module. An integrated circuit that securely stores an international mobile subscriber identity number and its related key. Used to identify and authenticate subscribers on mobile devices.
SMS - Short Message Service. A text messaging service for telephone, internet, and mobile device systems. It uses standardized communication protocols to let mobile phones exchange short text messages over cellular networks.
TCR - The Campaign Registry. An independent registry that acts as a centralized hub for registering 10-digit long code phone numbers and collecting brand and campaign data for Application-to-Person messaging.
Throughput - The measure of data transfer between connections as measured by message per second.
Vetting - The process of thoroughly investigating a brand, company, or other entity before making a decision to move forward with campaign registration.

Adrian Chavez Batta
The Campaign Registry
Vicepresident International Sales
Phone: +1 786 877 7767
Email: adrian.chavez@campaignregistry.com

Sheyla Rojo
The Campaign Registry
Senior Director, International Sales
Phone: +44 7548 237 916
Email: sheyla.rojo@campaignregistry.com

BETTER MESSAGING
campaign registry

1775 Tysons Blvd 5th floor, McLean, VA 22102
United States
www.campaignregistry.com