BETTER MESSAGING
campaign registry

HAVE YOUR SAY | 2024

SMS Sender ID Registry - Fighting SMS Impersonation Scams

Introduction

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

Operating under the umbrella of Tata Communications, a global leader in digital infrastructure and telecommunications, The Campaign Registry benefits from the company's extensive worldwide presence, with offices spanning across multiple countries, including Australia. This global reach enables The Campaign Registry to leverage Tata Communications' expansive network and expertise, ensuring seamless collaboration with carriers, messaging companies, and industry partners worldwide.

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

Operating at the heart of the messaging industry, The Campaign Registry collaborates closely with mobile operators and messaging companies to facilitate the registration of Application-to-Person text messaging campaigns. By offering visibility into messaging sources and content, the registry empowers mobile carriers to deliver a more dependable and straightforward service for Campaign Service Providers and brands alike.

In this introduction, we've highlighted the pivotal role of The Campaign Registry within global networks and its dedication to shaping the future of messaging campaign management with transparency, safety, and reliability at its core.

Definitions

- **A2P:** Application to Person.

- **API:** Application Programming Interface.

- **Brands:** The company or entity the End Customer believes to be sending the message.

- **Campaigns:** a set of attributes within a use case, which will reach the end user.

- **CNP:** Connection Network Provider

CNP’s provide the connection between the CSPs and the MNOs. Every CSP that registers with TCR is automatically added to the list of electable CNPs.

- **CSP:** Campaign Service Provider

The primary users of The Campaign Registry. As a CSP, you work with multiple Brands to create and launch their text messaging campaigns.

- **DCA:** Direct Connect Agreggator

DCA’s provide direct connectivity to the mobile carrier’s gateway for delivering messaging campaigns.

- **FW:** Firewall.

- **GW:** Gateway.

- **LC:** Long Code.

- **MNO:** Mobile Network Operator.

- **Phishing or Smishing** is an attack technique that tricks mobile network subscribers to share their personal or sensitive information such as credit card details.

- **SC:** Short Code.

- **Throughput:** The measure of data transfer between the connections measured by message per second.

- **Vetting:** The process of thoroughly investigating a brand or a company, or other entity before making a decision to go forward with a campaign registration in TCR.

• Have you, your organization, or clients been targeted by SMS impersonation scams that used your alphanumeric sender ID(s)?

TCR’s RESPONSE:

In many countries, The Campaign Registry (TCR), has been witness to scams and Sender ID manipulation. The industries which we have seen mostly impacted include those of:

- Banking
- Pension funds
- Insurance companies
- Government agencies
- Telecommunications companies
- Retail and e-commerce platforms
- Delivery and logistics services

TCR was created as a response to the current challenges being faced by partners and customers alike, and in turn prevents concerns such as brand impersonation, CLI manipulation, spoofing and artificially inflated traffic, amongst others.

Some of our preventative measures include (see attachment TCR Complete Deck 2024.pdf for our full service offering):

- Verification of businesses to ensure they are a legitimate company.
- Collection of legitimate sender IDs.
- Registration and visibility of brands and campaigns through portals and APIs which are integrated between stakeholders.
- Feedback loop, with real time reporting.

• Do you support the introduction of a voluntary or mandatory SMS Sender ID Registry for alphanumeric sender IDs? Why?

TCR’s RESPONSE:

Yes, TCR supports this initiative as a mandatory implementation. We believe that having a single national database with an exhaustive list of names and alphanumeric abbreviations to be used to identify the entities issuing the messages is a beneficial measure, provided it is done properly and linked to the technology behind it that can monitor the accuracy and legitimate participation of all the parties involved.

<u>Mandatory Registry:</u>

Based on our observations over the years and across the globe, cooperating with Regulatory Authorities and MNOs, the mandatory SMS Campaign Registry and Brand Registry is the only possible solution to prevent smishing fraud. TCR’s tried, tested, and proven approach has been instrumental in ensuring the legitimacy and safety of messaging to end users. Due to our global knowledge, we have found the following to be of importance:

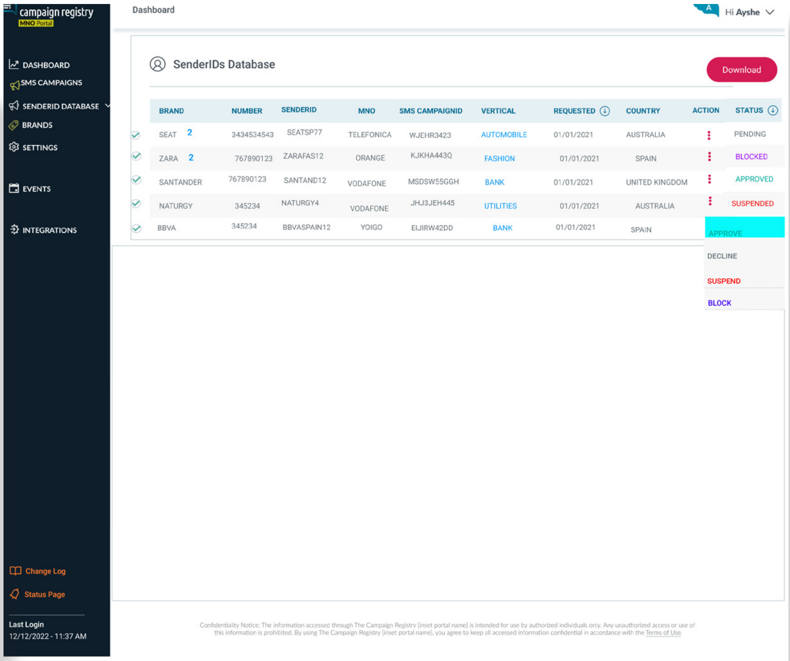
1. Mandatory registration ensures a single regulation norm in the country for every business, which instills confidence in recipients that businesses can never obtain SenderIDs without scrupulous verification by a government authorized body.

2. TCR encapsulates all key attributes of an SMS campaign such as Brand name, SenderID, sender number, SMS use case, industry, MNO name, Aggregator name in unique identifier, the CampaignID.

3. Mandatory SMS Campaign Registry and Brand Registry helps clean up the ecosystem from bad actors.

4. TCR works with the MNO's infrastructure, eg. Gateway and Firewall providers, to protect SenderIDs from CLI manipulation. This, coupled with a mandatory SenderID registry where key stakeholders are obligated to protect their networks from CLI manipulation ensures the success of such a solution.

5. Included in our approach is real-time visibility with options to suspend / block, tailored to each specific country's needs. In addition, the feedback loop is complete with monitoring and reporting functions.

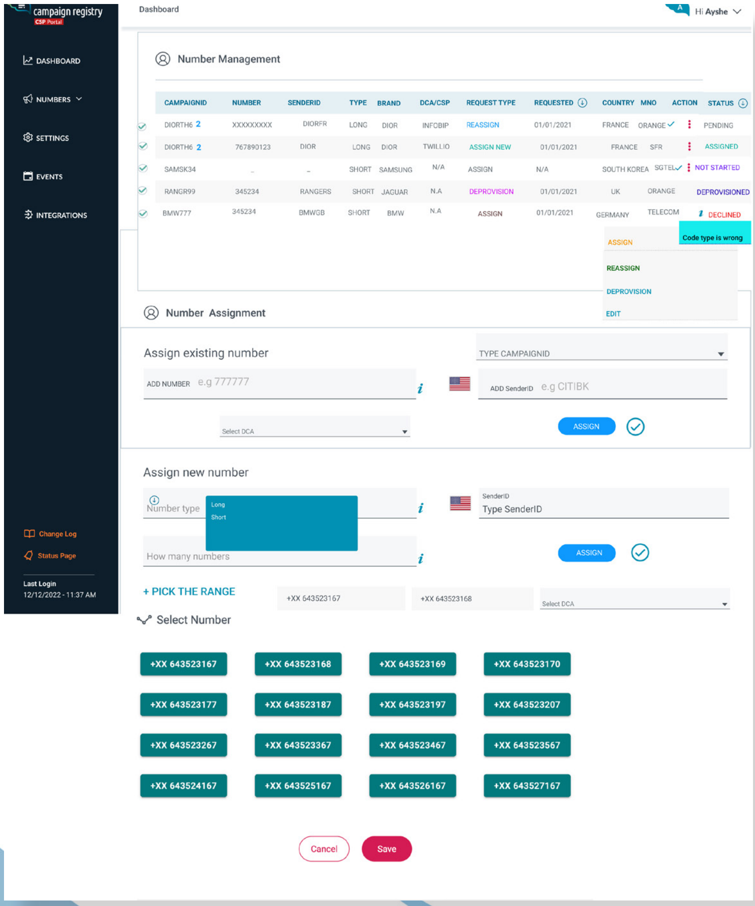


Last Login
12/12/2022 - 11:37 AM

SenderIDs Database

BRAND	NUMBER	SENDERID	MNO	SMS CAMPAIGNID	VERTICAL	REQUESTED	COUNTRY	ACTION	STATUS
SEAT 2	3434534543	SEATSP77	TELEFONICA	WJEHR3423	AUTOMOBILE	01/01/2021	AUSTRALIA	⋮	PENDING
ZARA 2	767890123	ZARAFAS12	ORANGE	KJKHA443Q	FASHION	01/01/2021	SPAIN	⋮	BLOCKED
SANTANDER	767890123	SANTAND12	VODAFONE	MSDSW55GGH	BANK	01/01/2021	UNITED KINGDOM	⋮	APPROVED
NATURGY	345234	NATURGY4	VODAFONE	JHJ3JEH445	UTILITIES	01/01/2021	AUSTRALIA	⋮	SUSPENDED
BBVA	345234	BBVASPAIN12	YOIGO	EIJIRW42DD	BANK	01/01/2021	SPAIN		

Confidentiality Notice: The information accessed through The Campaign Registry [inset portal name] is intended for use by authorized individuals only. Any unauthorized access or use of this information is prohibited. By using The Campaign Registry [inset portal name], you agree to keep all accessed information confidential in accordance with the Terms of Use.



Last Login
12/12/2022 - 11:37 AM

Number Management

CAMPAIGNID	NUMBER	SENDERID	TYPE	BRAND	DCA/CSP	REQUEST TYPE	REQUESTED	COUNTRY	MNO	ACTION	STATUS
DIORTH6 2	XXXXXXXXX	DIORFR	LONG	DIOR	INFOBIP	REASSIGN	01/01/2021	FRANCE	ORANGE ✓	⋮	PENDING
DIORTH6 2	767890123	DIOR	LONG	DIOR	TWILLIO	ASSIGN NEW	01/01/2021	FRANCE	SFR	⋮	ASSIGNED
SAMSK34	_	_	SHORT	SAMSUNG	N/A	ASSIGN	N/A	SOUTH KOREA	SGTEL✓	⋮	NOT STARTED
RANGR99	345234	RANGERS	SHORT	JAGUAR	N.A	DEPROVISION	01/01/2021	UK	ORANGE		DEPROVISIONED
BMW777	345234	BMWGB	SHORT	BMW	N.A	ASSIGN	01/01/2021	GERMANY	TELECOM	i	DECLINED

Code type is wrong

Number Assignment

Assign existing number

TYPE CAMPAIGNID

ADD NUMBER e.g 777777

ADD SenderID e.g CITIBK

Select DCA

Assign new number

Number type

SenderID
Type SenderID

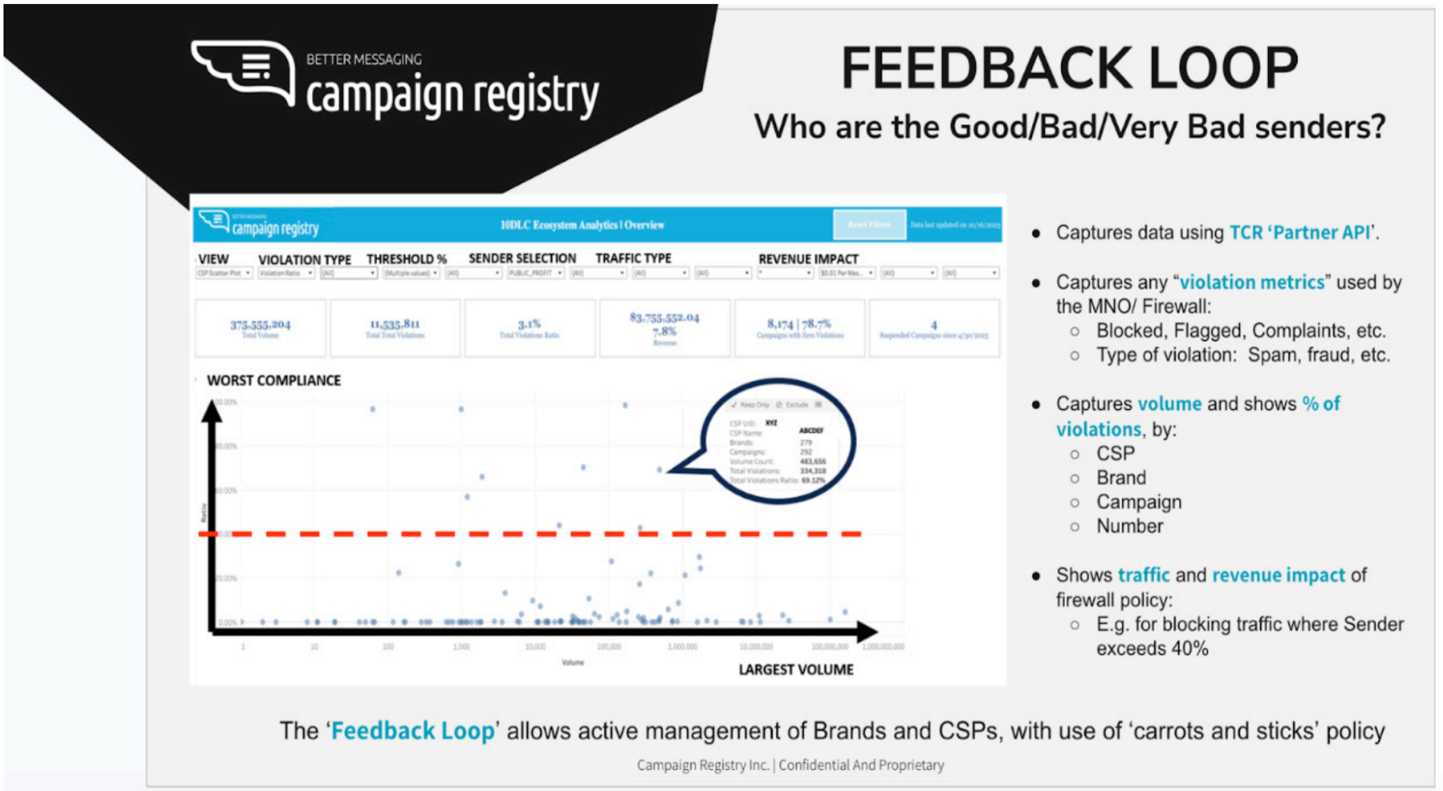
How many numbers

+XX 643523167 +XX 643523168 Select DCA

Select Number

+XX 643523167	+XX 643523168	+XX 643523169	+XX 643523170
+XX 643523177	+XX 643523187	+XX 643523197	+XX 643523207
+XX 643523267	+XX 643523367	+XX 643523467	+XX 643523567
+XX 643524167	+XX 643525167	+XX 643526167	+XX 643527167

Sender Number & ID Provisioning, Visibility, Traceability.



FEEDBACK LOOP

Who are the Good/Bad/Very Bad senders?

- Captures data using TCR 'Partner API'.
- Captures any "violation metrics" used by the MNO/ Firewall:
  - Blocked, Flagged, Complaints, etc.
  - Type of violation: Spam, fraud, etc.
- Captures volume and shows % of violations, by:
  - CSP
  - Brand
  - Campaign
  - Number
- Shows traffic and revenue impact of firewall policy:
  - E.g. for blocking traffic where Sender exceeds 40%

The 'Feedback Loop' allows active management of Brands and CSPs, with use of 'carrots and sticks' policy

Campaign Registry Inc. | Confidential And Proprietary

Voluntary Registry:

There have been attempts to create a "partial SMS Registry" in other countries across the globe. These lists are currently being used ineffectively, failing to prevent fraud with security concerns and gaps in its foundation at very high costs for the parties involved.

Our findings have noted the following challenges:

- Not all the aggregators and operators operating in the given country are part of the initiative, only a few are.
- There is no technology behind it as the process is purely manual and based on manual reporting in a spreadsheet or online dashboard.
- There are no checks or audits which confirm that the aggregators are actually protecting the sender IDs/brands and blacklisting them as expected. It is not a verified database.
- It is a limited solution, only available for 30-40 brands/merchants in a country at a high subscription cost. These are large companies and government agencies and the plan is to limit the reach therefore it is not an industry solution. The end users have continued experiencing spam and smishing at unprecedented levels also coming from other entities as there are thousands of brands/merchants in a country, therefore protecting only a few dozen would not have any sustainable or effective impact.
- The initiative relies on the parties' good diligence and trust, however when an issue arises, the damage is done and it has to be reactively remediated which also takes a significant amount of time. There is not a proactive solution available either. All the communications are manual with no log trails that could be used as evidence if/when required.

- There are also legal concerns about GDPR and data privacy given how the information is shared and the type of information requested. It is not an industry solution and it does not prevent fraud from happening.
- The cost is too high for the relevant parties.

TCR's existing Registry does/can act as a single, national database that supports the trace back from any single message to the full details of (1) the originating Brand, (2) the campaign in question, (3) the originating messaging platform, and if required also (4) the delivery path of them message if several messaging platforms are involved.

MNOs can check this database if the agent campaign is legitimate before sending messages. MNOs will also be able to block bad actors, preventing them from committing further spam/fraud and/or taking any other measures if/as needed.

TCR's Registry can act as a single national database of all the registered brands at a fraction of the cost with less resources required. TCR verifies the database and keeps it accurate in real-time. Our recommendation is, therefore, to onboard all participants as a mandatory solution. TCR enters into Data Licensing agreements with all ecosystem recipients of confidential information. TCR does not collect any PII data, but if needed separate Data Protection Agreements will be required, capturing also GDPR requirements.

What, if any, transition arrangements are required?

TCR's RESPONSE:

Rather than a transition, we believe that onboarding the players in the value chain is key to deploying a successful Registry. TCR already has the experience of onboarding all the stakeholders such as the MNOs, the CSPs, the Brands/Enterprises, DCAs and could assist with managing a numbering database if needed.

In the first 12 months, we onboarded more than 1350 aggregators, registered and verified over 3 million brands, completed integration with the four main MNOs in the US, and launched over 3 million campaigns, supporting over 5 billion SMS/MMS messages every month. Considering that most aggregators operating in Australia are already our partners and registered in Australia, alongside many international brands, we anticipate much quicker adoption and implementation.

The cost and impact are low in terms of effort from the current national infrastructure. A Registry like TCRs provides APIs, hence there are no modifications to the Networks platforms, the registry is also not in the path of the communication to avoid more hops and possible points of failure to the current communication channel. Also, having a Registry not involved in the path of the messages, the actual cost ($) shouldn't be tied to the current business model, that way the impact is also not considerable.

It is feasible to implement a solution like TCR, it's proven to be able to mitigate fraud and spam and also it has proven to onboard all stakeholders in the ecosystem quickly and safely.

A simple deployment solution could look as follows:

1. TCR would set up a phase-in approach with a clear roadmap, and optimal support from our dedicated team.

2. We would ensure a minimum time to market with little to no development costs since we are already operational in other countries. TCR is a fully fledged solution with 3 portals, backend architecture, SenderID database, and APIs up and running. We are already successfully functioning in the North American market, and currently in negotiations with other countries.

3. A clear deadline for mandatory registration would need to be established within Australia. Furthermore, all participants / stakeholders (CSPs, MNOs, brands) would need to comply on a contractual basis.

4. Of course, such an implementation would allow for a grace period, a timeframe to be agreed on. Thereafter, full compliance would take effect.

5. TCR would provide education and training on all aspects of registration, including that of our Registry Portals and APIs.

As previously mentioned, our current setup ensures that MNOs and Aggregators know everything about a message which is declared upon registration, eg. URL sample, brand, senderID. Should the MNO detect SMS whereby any part of the content does not correspond to that which was registered, the MNO may decide to block the SMS, SenderID or even the entire SMS campaign.

TCR however, goes beyond message content and SenderID protection. We may also protect MNOs from rogue aggregators, whose Artificially Inflated Traffic strategies, grey routes and other misuse scenarios deceive MNOs by cutting off their revenues and decreasing government's incoming taxes as a result.

Those discrepancies then are communicated with the MNO on TCR systems where MNO can take appropriate suspension/blocking actions.

On the next page are two examples of case studies, where a solution such as TCR's could have prevented the current outcome:

Australia

In January, A2P texting solutions company Modica received a warning for failing to comply with the rules. ACMA found Modica didn't have proper procedures to verify the legitimacy of text-based SMS sender IDs, which allowed scammers to reach many mobile users in Australia.

Had TCR's solution been implemented, TCR would have adopted responsibility for the verification and protection of said SenderIDs.

The registration would have undergone a stringent vetting process, including verification of:

- The sender/number
- The business entity
- The use case
- The message content

Ireland

In the last few months in Ireland , there have been multiple reports of SMS phishing attacks against account holders of one of the largest banks in Ireland -Bank of Ireland (BOI).
What is happening here is the sender address of the SMS – BOI – is being spoofed. 'BOI' sender is technically called an alphanumeric short code address, not a typical phone number address. It appears to be in the same thread as other, legitimate BOI communications, because when the handset receives messages from the same sender address, it places them in the same thread.

Had the Bank of Ireland's CSP registered its brand and A2P campaign with TCR, the "BOI" senderID would have been kept on record in TCR's database with the genuine sender number. The Firewall would have scanned the SMS to verify this against the database and check for SenderID - Sender number correlation. The Firewall would have scanned the message content for discrepancies and whether the SMS attributes were not those that had been initially registered. Had there been discrepancies, the MNO would have been signalled to potentially suspend the SMS campaign and warn the CSP.

Conclusion

These are the key actions required:

1. Register and verify brands.

2. Register and verify aggregators or service providers.

3. Register the attributes of the commercial action (SMS, RCS).

4. Define and set up use cases.

5. Register and associate the MSISDNs and Alphanumeric Sender IDs.

6. Establish a communication channel among all involved parties.

7. Enable suspension and complaint procedures for brands/campaigns violating MNO or regulatory guidelines.

8. Establish a feedback loop for analyzing and monitoring participant behavior.

In the Australian 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 a third-party entity independent enough 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 onboard all participants in the value chain, including brands, mobile network operators (MNOs), direct carrier aggregators (DCAs), communication service providers (CSPs), content network providers (CNPs), firewall providers, regulators, etc.

Implementing these measures, managed by TCR (for reference, TCR is already operational in the USA market, overseeing 10DLC SMS A2P campaigns), will significantly contribute to mitigating fraud in Australia.

[redacted]
The Campaign Registry
Vicepresident International Sales
Phone: +[redacted]
Email: [redacted]

[redacted]
The Campaign Registry
Sales Operations Senior Manager
Phone: +[redacted]
Email: [redacted]

BETTER MESSAGING
campaign registry

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