



GSMA Fraud Intelligence Service

User Guide v1.2

April 1, 2021

© Copyright 2021. GSM Association and/or its subsidiaries are the owners of GSMA High Risk Number Service and GSMA Fraud Intelligence Service trademarks, whether registered or unregistered, all rights reserved.

Table of Contents

1	INTRODUCTION	3
1.1	OVERVIEW.....	3
2	GETTING STARTED	4
2.1	LOG IN FOR THE FIRST TIME	4
2.2	RESET PASSWORD.....	5
3	HIGH RISK NUMBERS SERVICE	6
3.1	SUBMIT HIGH RISK NUMBERS	6
3.2	COLUMNS.....	7
3.3	VIEWS.....	9
3.4	DETAILS PAGE	10
3.5	DOWNLOAD HIGH RISK NUMBERS	11
3.6	NOTIFICATIONS.....	13
3.7	HELPDESK.....	14
4	GSMA FRAUD INTELLIGENCE SERVICE FULL SERVICE ACCESS	15
4.1	DASHBOARD	16
4.2	HIGH RISK NUMBERS.....	17
4.2.1	<i>Verification checks</i>	17
4.2.2	<i>Private comments and labels</i>	17
4.2.3	<i>Download High Risk Numbers</i>	17
4.2.4	<i>High Risk Ranges</i>	18
4.3	MOBILE NUMBER RANGES.....	19
4.4	MCC/MNC	20
4.5	OPERATOR IP RANGES	20
4.5.1	<i>Details Page</i>	21
4.6	API ACCESS	23
4.7	ALERTS & NOTIFICATIONS	24
4.8	SETTINGS & ADMINISTRATION.....	25
4.8.1	<i>Settings</i>	25
4.8.2	<i>Administration</i>	25
4.9	HELPDESK.....	27
4.10	ORGANISATION ROLES	28

1 Introduction

Welcome to the GSMA Fraud Intelligence Service User Guide.

This document serves to help prospective and approved GSMA operator member organisations to understand the process and resources required to use this service.

1.1 Overview

The GSMA Fraud Intelligence Service is a global platform, curating fraudulent telephone numbers and relevant IR.21 data collated from multiple primary sources – including our operator members. The platform enables real-time data exchange, as well as quick interrogation and validation to prevent costly network fraud. The system resides in Luxembourg, hosted by our service partner, RoamsysNext.

This User Guide begins with the free entry level of the GSMA Fraud Intelligence Service, **High Risk Numbers**, which is limited to three users per company account. It then moves on to describe the **Full Service** that's available on a subscription basis.

2 Getting started

2.1 Log in for the first time

Once users are approved by the GSMA, they will be emailed their temporary login credentials from RoamsysNext, to access either the full GSMA Fraud Intelligence Service or the High Risk Numbers free entry level, for the first time

If the username and password does not match, the system will display an error: 'Invalid Username / Password'.

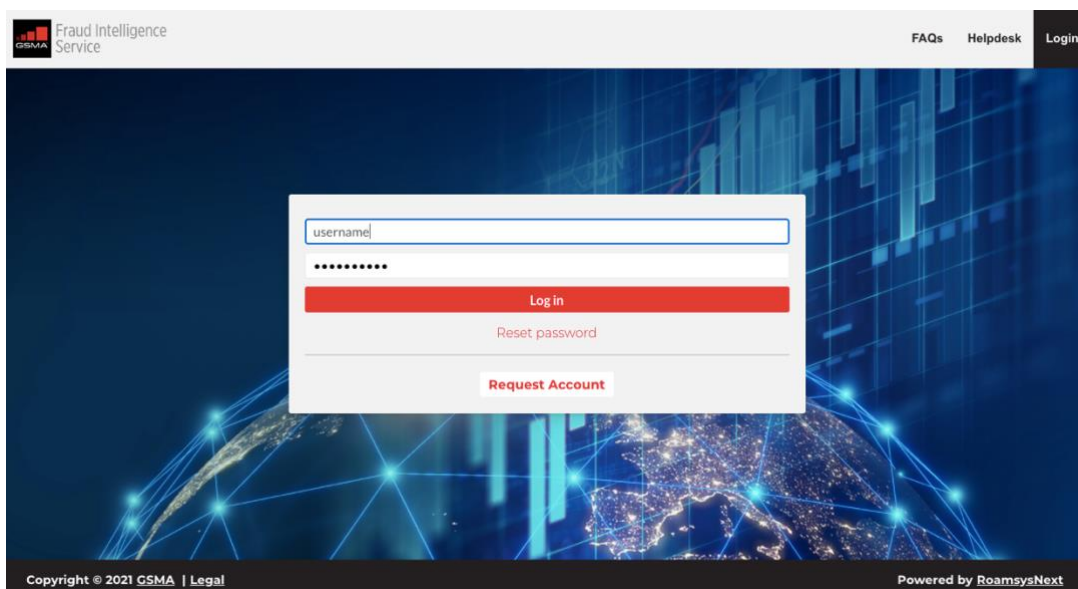


Figure 1: Login page

On successful authentication, the system will log in to the appropriate area of the platform. Either the **Full Service** or the **High Risk Numbers** overview page will be displayed.

2.2 Reset Password

Forgotten or lost your password? Reset it by selecting the Reset Password option from the login screen.

- **Go to the Fraud Intelligence Service login page.**
- **Click the Reset Password link displayed below the login form**
- **Enter your username and click “Request a new password”**

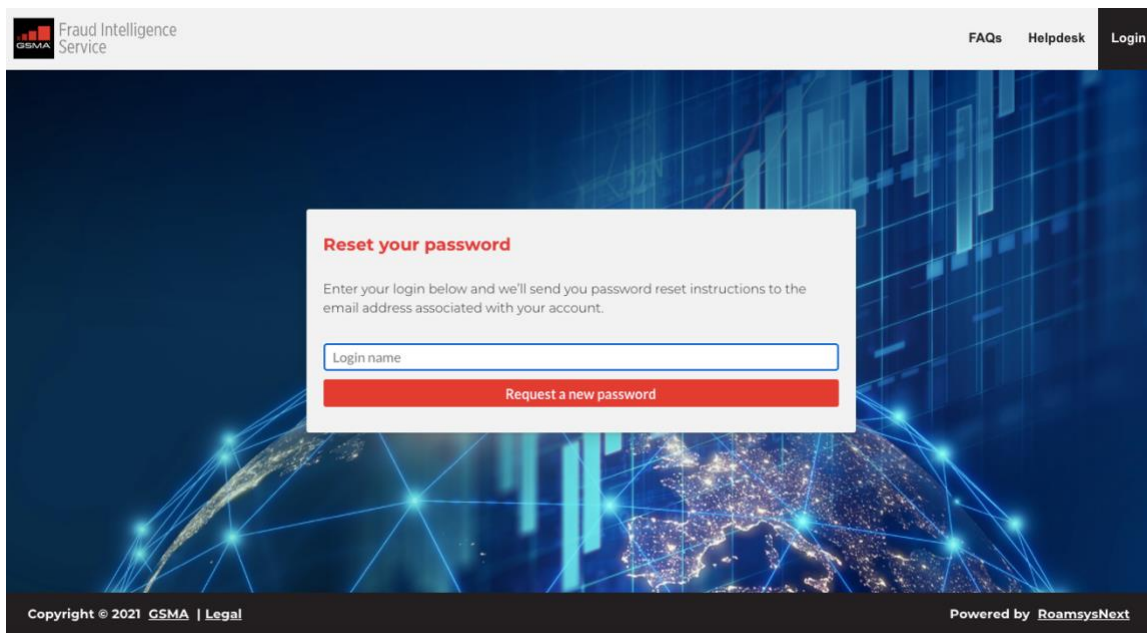


Figure 2: Reset Password

Once you submit the information, the system verifies the details and sends the reset password instructions, along with a link, to your registered email.

After you have activated your account, for return visits we suggest you bookmark your Login page at either <https://fis.gsma.com>.

3 High Risk Numbers Service

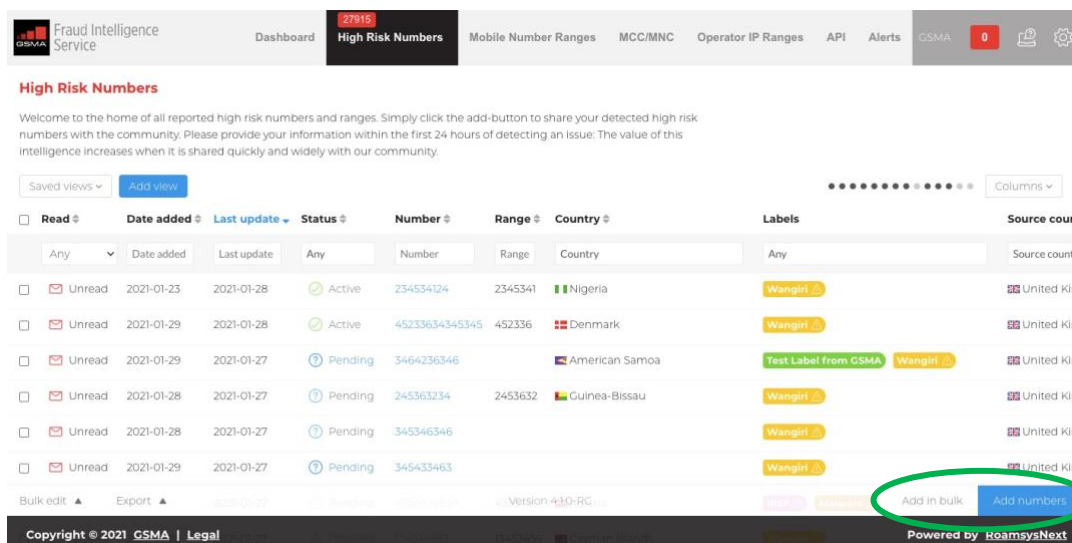


Figure 4: High Risk Number Service Page

The High Risk Numbers tab gives you a view of all the reported fraudulent numbers across multiple sources. Though the tabs for the full subscription service are present on the horizontal navigation bar, they are not active.

3.1 Submit High Risk Numbers

There are two ways to submit high risk numbers:

- To add numbers individually, click the Add numbers button on the bottom right of the page. A pop-up window will open for you to enter all required information: number, Fraud Label, status, Source TADIG and an optional comment.
- To add numbers in bulk, click Add in bulk and use the template provided to import large amounts of high risk numbers. Download the template and populate it with the relevant data you would like to share, and then upload it back into the system. If there is an error with the data, you will be presented with a summary list of the issues found. From this, you may Download an error report or cancel import from the navigation bar at the bottom of the page.

3.2 Columns

Click the **Columns** button, to hide/unhide any columns. Below is a list of all the categories you can use to filter the high risk numbers:

Read ⇅ Date added ⇅ Last update Status ⇅ Number ⇅ Range ⇅ Country ⇅ Labels
Last comment ⇅ Source country ⇅ Source organisation ⇅ Source TADIG ⇅ Sightings ⇅ Last sighting ⇅

Figure 5: Columns

Use the **Read** column to keep track of all the fraud numbers you have viewed. Tick the boxes and click on the **Bulk edit** button to change the status of a number. You will now easily notice the new fraud numbers as *Unread*.

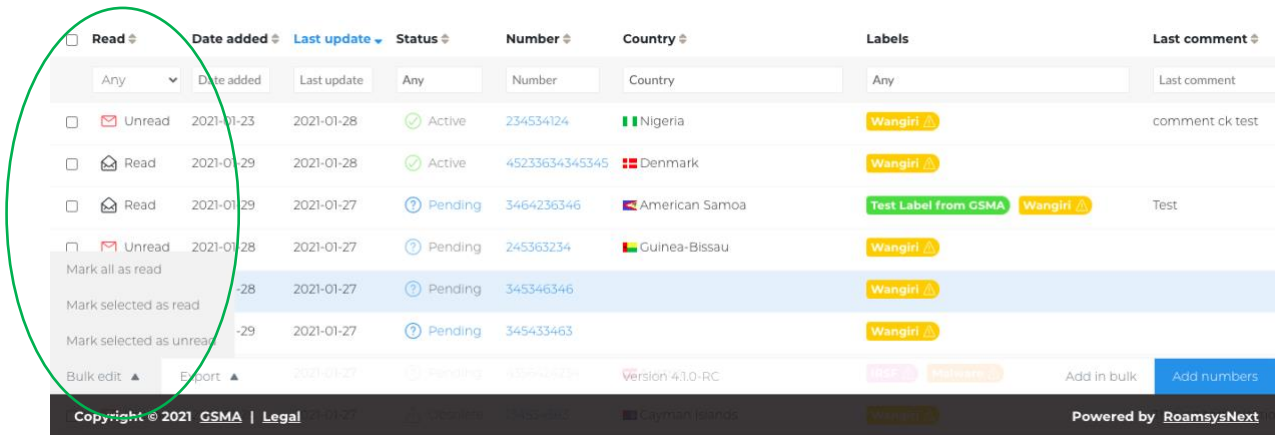


Figure 6: Mark Unread to Read

All columns can be filtered to find the information you are looking for. For example, try to look up recent High Risk Number alerts to your home country/network numbers. Use the **Date added** and **Country** or **Number** column filters to find if your country/network numbers have been under attack.

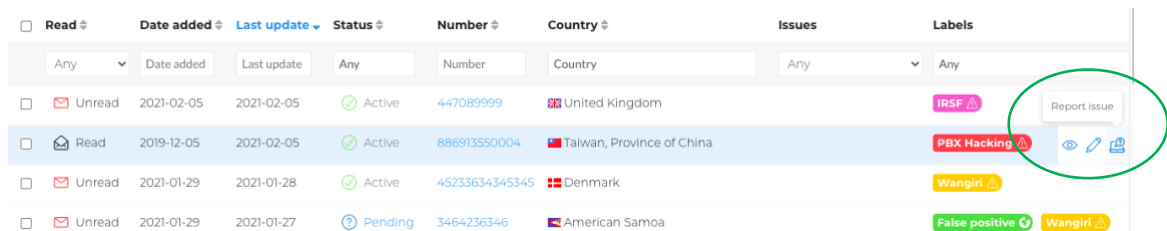
<input type="checkbox"/> Read	Date added	Last update	Status	Number	Country
<input type="checkbox"/> Any	<input type="text" value="Date added"/>	<input type="text" value="Last update"/>	<input type="text" value="Any"/>	<input type="text" value="Number"/>	<input type="text" value="Country"/>
<input type="checkbox"/> Unread	Date <input type="text" value="is"/>	<input type="text" value="2021-02-12"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Unread	2021-02-05	2021-02-05	<input checked="" type="checkbox"/> Active	447089999	United Kingdom
<input type="checkbox"/> Read	2019-12-05	2021-02-05	<input checked="" type="checkbox"/> Active	886913550004	Taiwan, Province of China

Figure 7: Filter on Date added

You can also view when an entry has had its **Last update**. This date will be used to understand which numbers need to be marked as obsolete. All reported high risk numbers are automatically attributed a **Status**. The categories for this are as follows:

Status	Description
Pending	A number or range that requires approval before publishing.
Active	Operators that have seen fraudulent traffic and have reported the numbers and ranges.
Excluded	Numbers that have been removed from the active list at the request of the number or range owner.
Obsolete	Fraudulent numbers that have not seen any activity in the last 18 months.

You can directly edit or remove the numbers added by your own organisation. However, if you find that your home network numbers are listed in the High Risk Numbers page and you know the numbers are wrong, or you notice any other error, click on the “Report issue” link in the rightmost of the row.



Read	Date added	Last update	Status	Number	Country	Issues	Labels
<input type="checkbox"/> Unread	2021-02-05	2021-02-05	Active	447089999	United Kingdom		IRSP
<input type="checkbox"/> Read	2019-12-05	2021-02-05	Active	886913550004	Taiwan, Province of China		PBX Hacking
<input type="checkbox"/> Unread	2021-01-29	2021-01-28	Active	45233634345345	Denmark		Wangiri
<input type="checkbox"/> Unread	2021-01-29	2021-01-27	Pending	3464236346	American Samoa		False positive, Wangiri

Figure 8: Report Issue

The **Country** column identifies which country the number belongs to and is determined by the Country Code (CC).

Search by **Label** (e.g. Wangiri), to find relevant fraud alerts. Labels are assigned when the High Risk Number is uploaded.

To see more info on any given High Risk Number, add a label or leave a comment, simply open its detail view by clicking directly on the number (or on the “details” link).

Last comment gives you the date the last comment within the details of that entry was made.

The next three, **Source Country**, **Source Organisation** and **Source TADIG** code all relate to the organisation that submitted the HRN entry.

The **Sightings** column is a tallied number of all the sightings for that entry, the **Last Sighting** gives you a date of when this entry was last seen in a fraudulent event.

3.3 Views

Click on **Add view** to save all selected column filters as a bookmark. Simply click on the saved bookmark the next time you visit the page and apply all the previously

selected filters with one click. Or save the selected filters as a default view to be displayed every time you return to this page.

High Risk Numbers

Welcome to the home of all reported high risk numbers and ranges. Simply click the add-button to share your detected high risk numbers with the community. Please provide your information within the first 24 hours of detecting an issue: The value of this intelligence increases when it is shared quickly and widely with our community.

Saved views ▾ **Add view** Columns ▾

Read	Date added	Last update	Status	Number	Country	Labels	Last com
<input type="checkbox"/>	Unread	2021-02-05	2021-02-05	Active	447089999	United Kingdom	IRSF
<input type="checkbox"/>	Read	2019-12-05	2021-02-05	Active	886913550004	Taiwan, Province of China	PBX Hacking

Figure 9: Add view

You can set different views of the columns you have visible. Click **Add view** and it will appear under your **Saved views**.

3.4 Details Page

High risk number details for 12462598012

Reports

Community

Date added	Last update	Status	Country
2021-02-23	2021-02-23	Active	Barbados

Sightings

1 sighting [Add sighting](#)

Labels

Fraud labels: IRSF

Global labels

Comments

[Add global comment](#)

Reported by GSMA 23 February

Version 5.0.0-RC

Copyright © 2021 GSMA | Legal Powered by RoamsysNext

Figure 10: HRN details page

The **Reports** section covers all reporting of this number as submitted within the community.

You may upvote on **Sightings** within this page.

Your **comment** will be shared with all users of the platform, by clicking **Add global comment** button to share your findings.

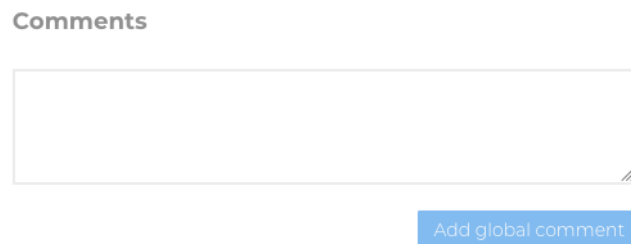


Figure 11: Add Comment

3.5 Download High Risk Numbers ↓

Users may download a list of the High Risk Numbers monthly via CVS or Excel by clicking the related format via the Export button at the bottom of the page. The export works on a “what you see is what you get” basis, so if you filtered results only the visible entries will be downloaded.

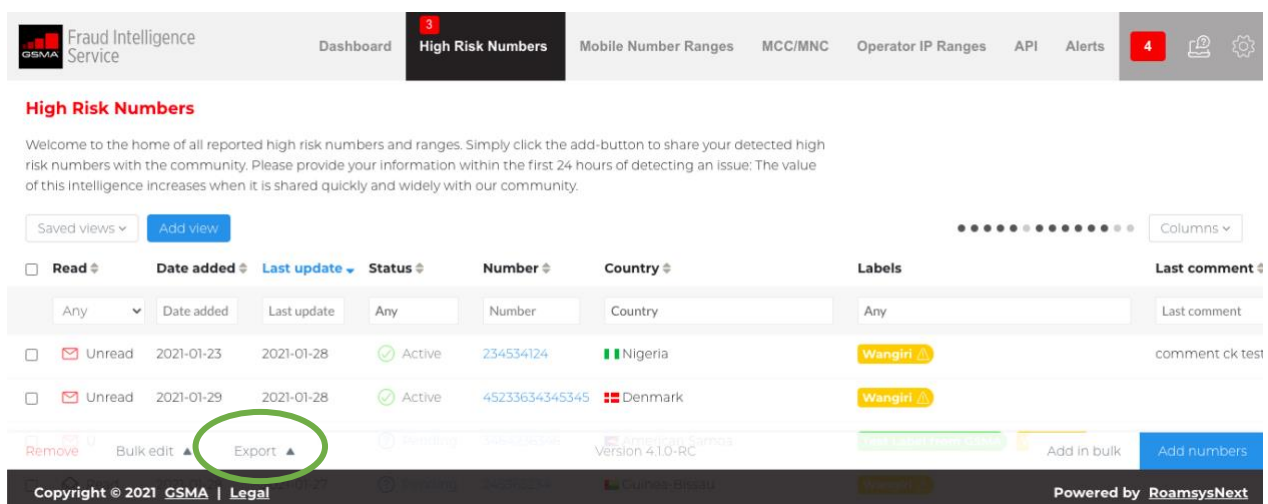


Figure 12: Export High Risk Numbers

If you would like to download the numbers more frequently, you will be required to contribute. Then from the time you contribute, you can download the HRN once within the following 24 hours.

To download High Risk Numbers more frequently, we ask operators to contribute their data on a more regular basis. For every contribution made, you will be able to download your picked numbers within the following 24 hours.

The full subscription services offers access to the High Risk Numbers, 24/7, irrespective of your contribution. Email: FraudIntelligence@gsma.com for more information.

3.6 Notifications

Alerts are signposted above the GSMA Fraud Intelligence Service top horizontal navigation bar within red boxes. The number in the red box appears over the HRN tab to indicate the number of updates or unread entries posted since the user last checked into that area.

TIP – on first entry to High Risk Numbers, you may mark all, as unread, so new entries are highlighted and obvious to you when you next log in.

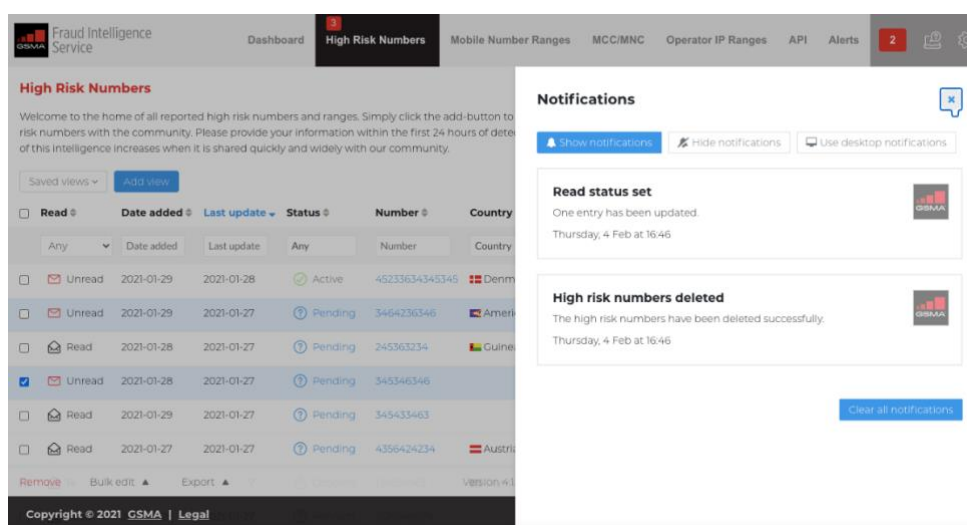


Figure 13: Notifications

The red box, to the right of your organisation name, flags the notifications that inform you of the following types of actions: update labels, add a comment, delete a comment, etc.

Within the notifications box, you can choose from the following options:

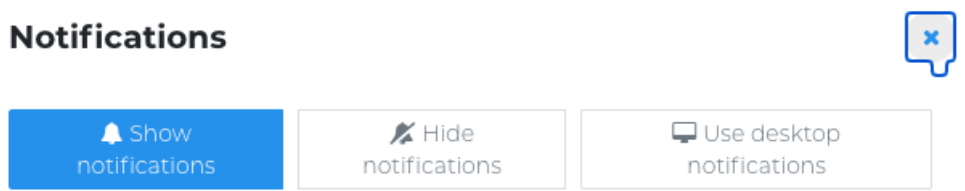
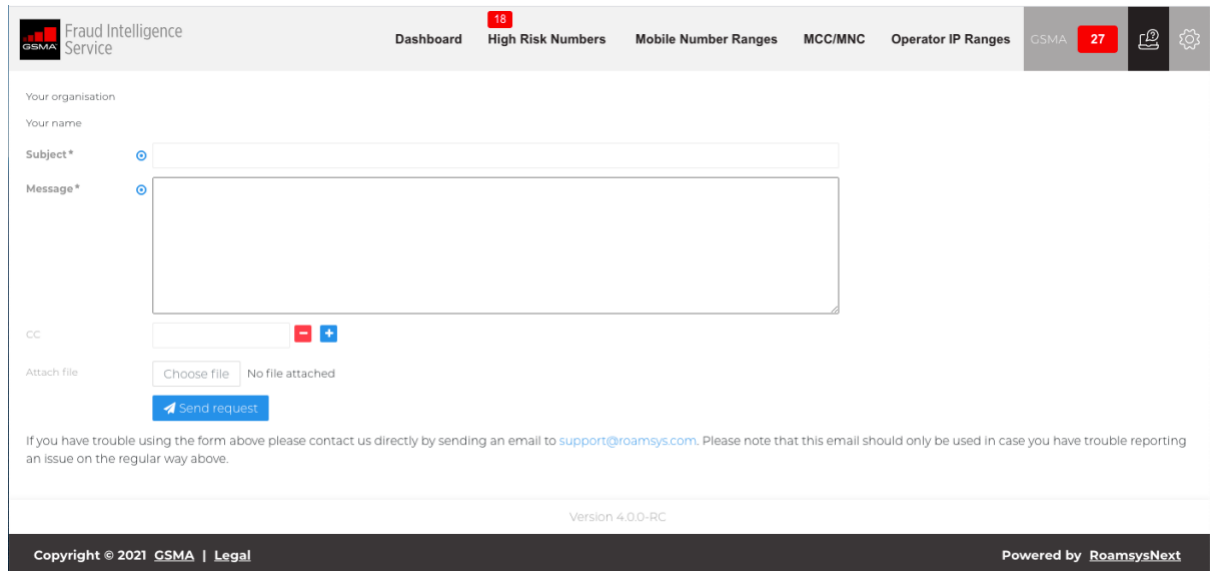


Figure 14: Notification options

3.7 Helpdesk

For technical or data-related support, there's a contact form on the helpdesk page.



The screenshot shows the 'Fraud Intelligence Service' helpdesk interface. The top navigation bar includes 'Dashboard', 'High Risk Numbers' (with a red notification badge '18'), 'Mobile Number Ranges', 'MCC/MNC', and 'Operator IP Ranges'. On the right, there is a 'GSMA' logo with a red notification badge '27' and a settings gear icon. The main form area contains the following fields:

- 'Your organisation': A text input field.
- 'Your name': A text input field.
- 'Subject*': A text input field with a blue circular icon to its left.
- 'Message*': A large text area with a blue circular icon to its left.
- 'CC': A text input field with a red minus sign and a blue plus sign to its right.
- 'Attach file': A 'Choose file' button and the text 'No file attached'.
- 'Send request': A blue button with a white arrow icon.

Below the form, there is a note: 'If you have trouble using the form above please contact us directly by sending an email to support@roamsys.com. Please note that this email should only be used in case you have trouble reporting an issue on the regular way above.'

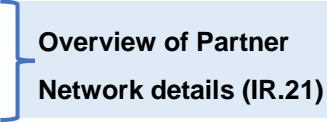
At the bottom of the page, the footer contains 'Version 4.0.0-RC', 'Copyright © 2021 GSMA | Legal', and 'Powered by RoamsysNext'.

Figure 15: Helpdesk Message Form

For any further questions, please contact the Fraud Intelligence Service team using the following email: FIShelpdesk@gsma.com.

4 GSMA Fraud Intelligence Service Full Service Access

The following sections are accessible for users of the full subscription service:

- **Dashboard**
 - **High Risk Numbers**
 - **Mobile Number Ranges**
 - **MCC/MNC**
 - **Operator IP Ranges**
 - **API**
 - **Settings & Administration**
 - **Report distribution**
 - **Helpdesk**
- 
- Overview of Partner
Network details (IR.21)

4.1 Dashboard

The dashboard functionality allows you to get an overview of your database, and monitor reported fraud numbers as well as IP (Internet Protocol) range threats on a world map.

All information is customisable and can be configured by each user. To customise any dashboard gadget, click on the pencil icon. There you can apply heat map settings, and choose if the countries who reported the fraud, or the countries of the called fraud numbers itself, will be visualized on the threat map.

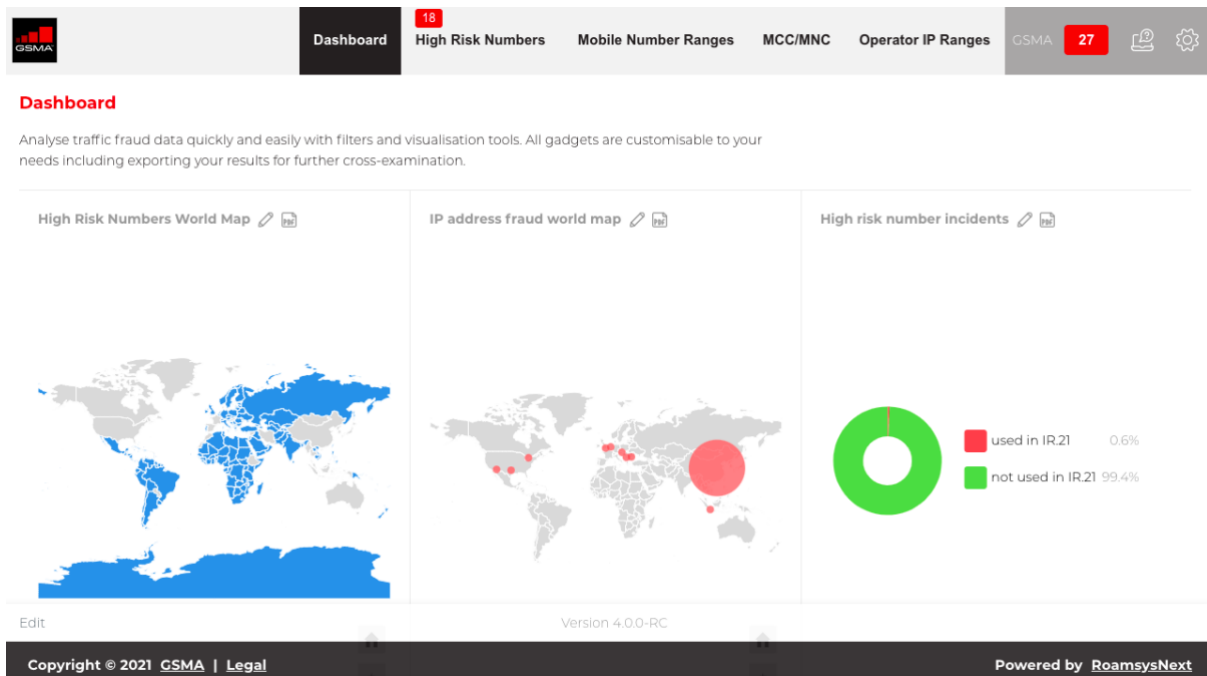
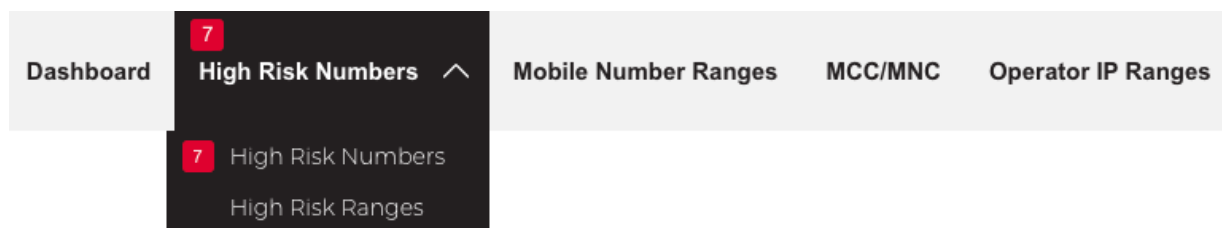


Figure 16: Dashboard

4.2 High Risk Numbers



The **Full Service** includes everything mentioned in the High Risk Numbers service (see page 6), plus all the following.

4.2.1 Verification checks

Each reported number is checked automatically against the GSMA IR.21 database to detect if it belongs to any of your partner networks. “Partner range match” warning will be displayed in the **Issues** column if a match is detected. This can speed up blocking of the fraud numbers and ensure that valid partner network ranges will not get blocked. You can also define CC/NDC priority ranges in the administration to get “Partner range match” warnings.

See the **Checks** section on details view to find all the matching partner networks and subsections where the range is defined. E.g. to discover hijacked MSRN ranges.

4.2.2 Private comments and labels

You can use private comments and labels to share information only with colleagues. You may add additional **Labels** within the details page. For further information on how to create labels, please look at the settings page.

4.2.3 Download High Risk Numbers

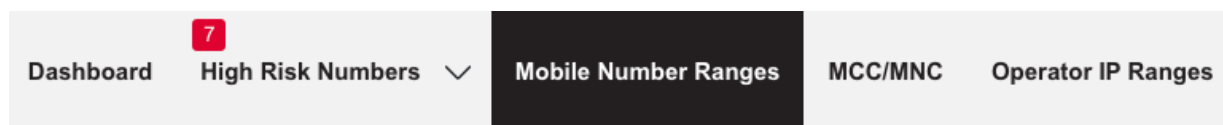


The full subscription services offers 24/7 access to the High Risk Numbers, irrespective of your contribution. Please refer to page 13 and the High Risk Numbers Download section to understand how to perform this task.

4.2.4 High Risk Ranges

In addition to the High Risk Numbers overview there is a High Risk Ranges overview that shows a summary of all high risk numbers per range. The High Risk Ranges overview can be reached via the dropdown menu in the main navigation bar or via the link in the **Range** column.

4.3 Mobile Number Ranges



The mobile number ranges page displays all partner network number ranges from IR.21 documents. If suspicious traffic from a particular number is detected, the source operator and history of the number range can be investigated.

This section allows you to:

- **View number ranges and Global Titles from IR.21 across your partners.**
- **View each number range record for data conflicts, and compare against reported fraud alerts.**
- **Run customisable duplicate checks across your partner network documents.**

See the **Issues** column to find all the validation check results, and if there are, any matching fraud numbers reported that fall under any given number range.

Go to **Detail view** to see more info for any given number range, add Label or leave a Comment.

The screenshot shows the 'Mobile Number Ranges' page. At the top, there's a navigation bar with 'Dashboard', 'High Risk Numbers' (7), 'Mobile Number Ranges' (active), 'MCC/MNC', 'Operator IP Ranges', and a notification badge '12'. Below the navigation bar, there's a section titled 'Mobile Number Ranges' with a descriptive paragraph. Underneath, there are 'Saved views' and 'Add view' buttons. An 'Advanced Table Filter' is present with various criteria like 'Connection type', 'Own TADIG code', etc. The main part of the page is a table with columns: 'Effective', 'Country', 'Operator', 'TADIG code', 'Tags', 'CC', 'NDC', and 'SN range'. The table contains three rows of data.

Effective	Country	Operator	TADIG code	Tags	CC	NDC	SN range
2020-11-16	United Kingdom	***Test RAEX Operator A	ROAM1	Premium UK	1	2	30000
2020-11-16	United Kingdom	***Test RAEX Operator A	ROAM1	Premium UK	355	672	600020
2020-08-08	United Kingdom	***Test RAEX Operator A	ROAM1	Premium UK	213	770	476560

Figure 17: Mobile Number Ranges

4.4 MCC/MNC

Look up mobile country codes, mobile network codes, MGT ranges and EPC realms.

MCC/MNC

Here IR21 data across all of your partner networks can be easily accessed. Check IMSI codes, MGT ranges, EPC realms and APNs across all relevant IR.21 subsections.

Advanced Table Filter Connection type: Any - Own TADIG code: Any - Direction: Any - Service: Any - Status: Any

Effective	Country	Operator	TADIG code	MCC/MNC	Tags	MGT CC/NC	IMSI
2020-08-08	United Kingdom	***Test RAEX Operator A	ROAM1	123 456	Premium UK	834 934	123441
2020-08-08	United Kingdom	***Test RAEX Operator A	ROAM1	123 456	Premium UK	834 934	123442
2020-08-08	United Kingdom	***Test RAEX Operator A	ROAM1	123 456	Premium UK	834 934	123443

Figure 18: MCC/MNC

Under this tab, IR.21 data across all of your partner networks can be accessed, including:

- Look up MCC/MNC aka IMSI (International Mobile Subscriber Identity) ranges across all IR.21 sections.
- Find and report EPC (Evolved Packet Core) realms and APN's of data roaming partners.
- Use MGT (E.214 CC/NC) column data to validate inbound roaming service configurations.
- Find sub range IMSIs if specified in IR.21 document.

4.5 Operator IP Ranges

The **Operator IP Ranges** page provides an overview of mobile operator IP ranges, together with IP look-up and data validation results.

- IP ranges from all IR.21 sections across all your partners.
- IP look-up results that are updated daily.

- **Each IP address is validated against threat feeds.**
- **Customise duplicate checks across all your partner networks.**

See the **Issues** column to find all the checks results. The red cross indicates issues that match to this record.

In the first **MCC/MNC** column, IR.21 document owner metadata is shown. This is the first and main guide to follow. An additional MCC/MNC column is provided based on the IP look-up results. It displays the operator who has registered the IP range (displayed only if matching operator and MCC/MNC is detected).

4.5.1 Details Page



To see all available information on any given IP range record, open the **details page** by clicking directly on the IP address field (or on the details link). In the upper left you can find all the subsections where this IP record is listed in the IR.21 document. Expand the **Checks** box below to find all the validation check results.

- **On the right-hand side you can find all your commercial connections with the partner network.**
- **Find the full details of the IP look-up results: ASN (Autonomous System Number) information and exact location on the map where the IP is registered.**
- **You can add Labels to each record. Private labels will be visible to your home organisation only.**
- **Leave a private Comment to users in your organisation.**

TIP: To find all the GRX IP backbone ranges from all your data roaming partner networks filter the report by the **Subsection**: “Connection to inter-PMN IP backbone” and tick only the data services in the **Connections** column filter (or click on the Advanced Table Filter pencil icon above the table to define more granular footprint filters).

TIP: To share data or continue analysing it offline, click on the “Export” button in the lower left corner to export data from any overview as Excel or CSV.

By default, information from the most recent IR.21 document is displayed. To look up historic data from obsolete entries, you should first unhide the **Ineffective** column to define the time periods of the data archive that you would like to view.

The screenshot displays the 'Operator IP Ranges' section of the GSMA Fraud Intelligence Service. At the top, there's a navigation bar with 'Dashboard', 'High Risk Numbers' (with a red notification badge '16'), 'Mobile Number Ranges', 'MCC/MNC', and 'Operator IP Ranges' (with a red notification badge '27'). Below the navigation bar, the page title 'Operator IP Ranges' is followed by a brief description: 'Here the IP-information across all of your partner networks can be easily accessed. The IR.21 data is enriched with geolocation, ASN data, threat detection and reported incidents from ipdata. Create intelligent data to support fraud detection decision making. The issues column displays all data conflicts to prompt further investigation.' Below this, there are buttons for 'test', 'Saved views', and 'Add view'. The main content area features an 'Advanced Table Filter' with various criteria like 'Connection type', 'Own TADIG code', 'Direction', and 'Service'. A table of data is shown with columns: 'Effective', 'Country', 'Operator', 'TADIG code', 'MCC/MNC', and 'Tags'. A filter dropdown is open over the table, showing options for 'Check All', 'Check None', 'Effective', 'Ineffective', and 'Country'. A green arrow points to the 'Columns' dropdown menu, which is used to toggle the visibility of the 'Ineffective' column. The table shows several rows of data, all with 'Effective' status and 'United Kingdom' as the country. At the bottom, there's an 'Export' button and a footer with 'Copyright © 2021 GSMA | Legal' and 'Powered by RoamsysNext'.

Figure 19: Operator IP Range – Filter to look up obsolete entries

4.6 API Access

The API delivers all information that is visible in this application. It is available for all subscription GSMA Fraud Intelligence Service customers, all the technical data you require is in the GSMA Fraud Intelligence Service API Specification document, available through the FIshelpdesk@gsma.com.

There are API calls for each main section of the application:

- High Risk Numbers
- Mobile Number Ranges
- Operator IP Ranges
- MCC/MNC

For each main section, there are three API calls (more to come in the future):

- metadata: get metadata (e.g. status values, labels or fraud types)
- all: get all items (e.g. fraud numbers, IP addresses)
- Find By____: get information for a specific item (e.g. a single fraud number or IP address)

For high risk numbers there are additional calls to add, delete and comment on high risk numbers.

4.7 Alerts & Notifications

Alerts are signposted above the GSMA Fraud Intelligence Service top horizontal navigation bar within red boxes. The number in the red box appears over a specific tab to indicate the number of updates posted since the user last checked into that area.

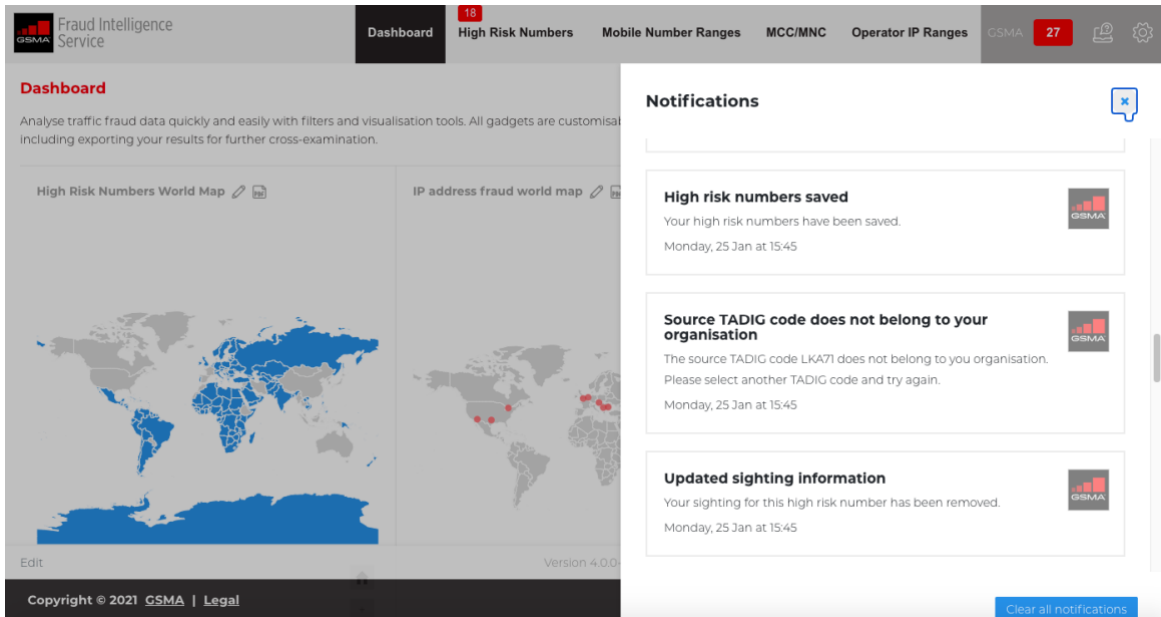


Figure 20: Notifications

The red box, to the right of your organisation name, flags the notifications which inform you of all the actions taken on the platform. You can **clear your notifications** by clicking the blue button at the bottom of the box.

Within the notifications box, you can choose from the following options:

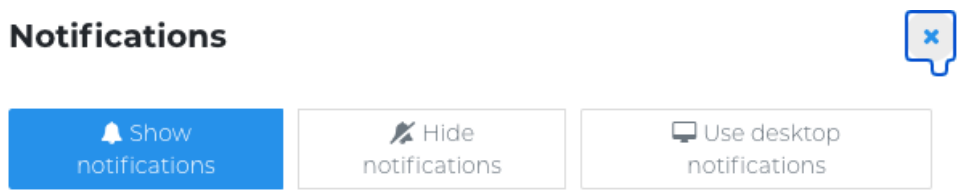


Figure 14: Notification options

4.8 Settings & Administration

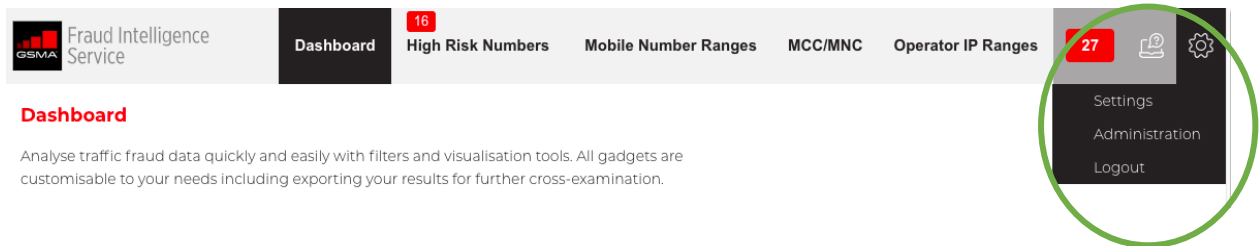


Figure 22: Administration

4.8.1 Settings

The settings page allows you to customise your personal start-up page, from any of the tabs as options.

4.8.2 Administration

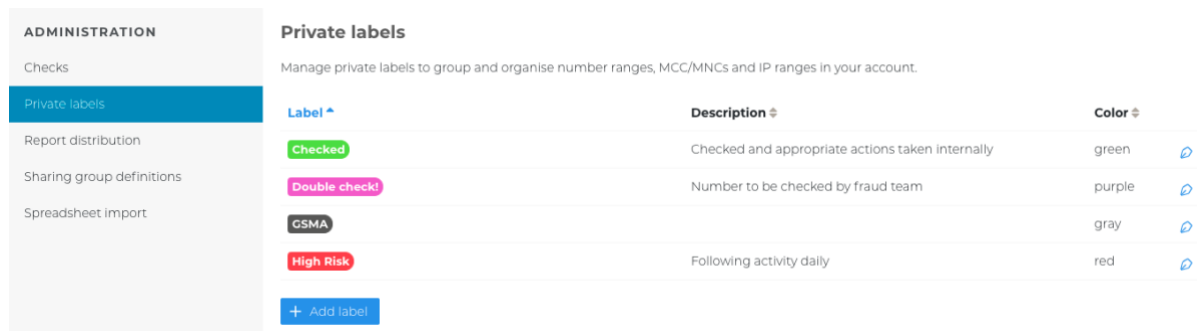


Figure 23: Private Labels example

Here users can change the behavior of the application.

Checks:

- Define CC/NDC values to check if high risk numbers fall under priority number ranges.
- Allow duplicate checks look for IP address and number range duplicates. Exceptions from the duplicate checks can be allowed.
- Limit IP address duplicate check based on specific subsections. To focus on relevant issues you can limit your duplicate check compare base, e.g. compare only backbone IP address ranges.

- Limit number range duplicate check based on specific subsections. To focus on relevant issues you can limit your duplicate check compare base, e.g. compare only GT (Global Title) number ranges.

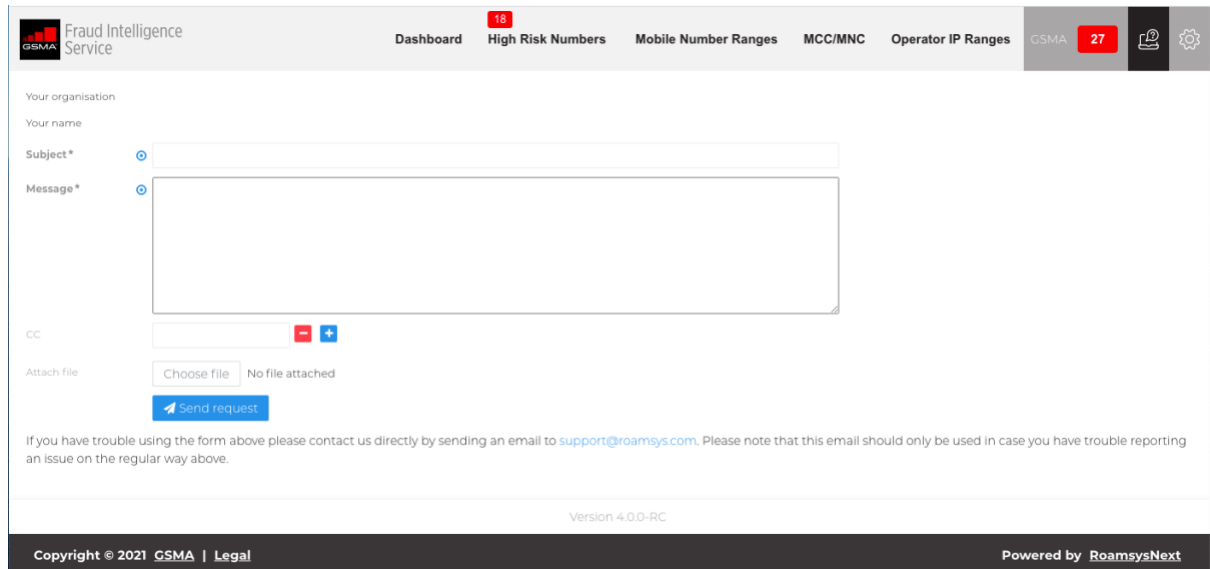
Private labels: Manage, add and edit

Report distribution: Set reports to be automatically emailed or uploaded to a remote server on a custom schedule. You may also define reports that are based on any view that has been saved on a supported page.

Sharing group definitions: Have a look at the sharing groups and define additional sharing groups to reduce duplicate checks only to relevant issues when operators share the same number ranges and IP ranges.

4.9 Helpdesk

For technical or data-related support, there's a contact form on the helpdesk page.



The screenshot shows the FIS helpdesk contact form. At the top, there is a navigation bar with the GSMA Fraud Intelligence Service logo on the left and several menu items: Dashboard, High Risk Numbers (with a red notification badge '18'), Mobile Number Ranges, MCC/MNC, Operator IP Ranges, GSMA (with a red notification badge '27'), and a user profile icon with a settings gear. Below the navigation bar, the form is titled 'Your organisation' and includes fields for 'Your name', 'Subject*' (with a dropdown arrow), and 'Message*' (with a dropdown arrow). There is also a 'CC' field with a dropdown arrow, a red minus sign, and a blue plus sign. An 'Attach file' section contains a 'Choose file' button and the text 'No file attached'. A blue 'Send request' button is located below the form. A note at the bottom of the form reads: 'If you have trouble using the form above please contact us directly by sending an email to support@roamsys.com. Please note that this email should only be used in case you have trouble reporting an issue on the regular way above.' The footer of the page includes 'Version 4.0.0-RC', 'Copyright © 2021 GSMA | Legal', and 'Powered by RoamsysNext'.

Figure 15: FIS helpdesk

For any further questions, please contact the Fraud Intelligence Service team using the following email: FIShelpdesk@gsma.com.

4.10 Organisation Roles

Overview of Organisation Roles:

Role:	Assign user roles	Submit	Edit	Read
Main Contact	X	X	X	X
Edit		X	X	X
Read Only				X