

CTIA IN-MARKET MONITORING PORTAL

USER GUIDE

CONTENTS

- Logging into the CTIA IMM Portal..... 1
- Requesting Login Credentials 1
- Navigating the CTIA IMM Portal 1
- Contacting the CTIA Support Team 3
- Program Violation Notices..... 4
 - Responding to Audits through the CTIA IMM Portal 4
 - Responding to Audits via Email 5

CTIA IN-MARKET MONITORING PORTAL

USER GUIDE

The CTIA In-Market Monitoring Portal (CTIA IMM Portal) is a Web-based environment designed to help content providers, aggregators, carriers, and CTIA–The Wireless Association® (the CTIA) manage the compliance of PSMS campaigns. If you work in the PSMS industry, you can access audits issued on behalf of your company in this searchable database. The functionality of the CTIA IMM Portal features advanced filters for all types of advertising and message flow. You also can download your search results in CSV format.

LOGGING INTO THE CTIA IMM PORTAL

Logging into the CTIA IMM Portal is simple. To gain access:

- Go to <http://ctia.psmsindustrymonitor.com/user/login>,
- Enter your login credentials in the Username and Password fields,
- Type the two CAPTCHAs, and
- Click the Login button.

A program violation notice can be accessed by the content provider and aggregator or aggregators of record for the associated shortcode. All carriers and the CTIA also can access program violation notices. If your username is correct but you're having trouble accessing the portal, try resetting your password using the Request a Password Reset link below the Login button on the CTIA login screen.

REQUESTING LOGIN CREDENTIALS

The Request a Password Reset link leads to a screen with fields for entering your username and email address. Enter the information associated with your CTIA IMM Portal account. Multiple email addresses can be associated with a single username, but for the password reset function to work, only one email address must be entered in the email field.

If you encounter problems on this screen, call (855) 272-8182 or email support.ctia@psmsindustrymonitor.com for help.

NAVIGATING THE CTIA IMM PORTAL

The CTIA IMM Portal interface has been designed for clarity and user-friendliness. Relatively intuitive, navigation involves horizontal tabs customized to your level of user access. Content providers, aggregators, and carriers have access to one primary page, via the Audit Search tab. The CTIA, along with carriers that deploy carrier-specific monitoring and reporting solutions based on CTIA audit data, have access to a Statistics tab.

Via the Audit Search tab, you can look for specific audits using the following search parameters:

Publication Dates: This function allows you to set a date range in which to search. Several preset date ranges are loaded into the dropdown menu accessible inside the text-entry field. Or, you can enter a custom range by typing two dates separated by a dash in the following format: YYYY/MM/DD-YYYY/MM/DD.

Audit Status: An audit may exist in one of six potential statuses: Open, Pending Retest, Retest Failed, Escalated, Closed, or Withdrawn. Exhibit 1 defines the audit statuses and indicates who’s responsible for taking action on the audit in each status.

Exhibit 1. Audit Status: What It Means and Who Must Act

Status	Definition	Who Must Act
Open	CTIA Compliance Team is awaiting communication from the responsible aggregator (AG) or content provider (CP) until the cure date.	AG or CP
Pending Retest	Responsible AG or CP has advised the Compliance Team of a reasonable estimated fix date.	Compliance Team
Retest Failed	Compliance Team has performed a scheduled retest, which has failed.	AG or CP
Escalated	Cure date has passed with no communication from the responsible AG or CP regarding the audit or maximum number of retest requests has been exceeded.	CTIA or Carriers
Closed	Audit is closed.	N/A
Withdrawn	Audit is withdrawn.	N/A

Severity: This function filters by audit severity (e.g., show only audits designated Severity 1).

Association: This function filters by the CTIA or by carrier for carriers that deploy carrier-specific monitoring and reporting solutions based on CTIA audit data.

Network: This function refers to the handset on which a service was tested or to the network applicable to the audit when the Network and the Association differ (e.g., Industry audits display the Association “CTIA,” while a message flow test conducted on a specific carrier handset will additionally list a specific Network, such as “Sprint”). Industry advertising audits, performed for all participating carriers, display “Cross-Carrier” in the Network dropdown menu.

Aggregator: This function filters by aggregator (e.g., show only audits that pertain to mBlox).

Content Provider: This function filters by content provider (e.g., show only Flycell audits).

Shortcode: This function filters by shortcode (e.g., show only audits of ads and message flows associated with 12345). Shortcode options appear in a dropdown menu once you begin entering the shortcode in the Shortcode field.

Products: This function filters by product type. You may select as many products simultaneously as you wish by ticking the appropriate checkboxes in the dropdown menu (e.g., show only Standard Rate Advertising audits; show only Premium Advertising and Premium Message Flow audits).

Audit Number: This function allows you to search for a single known audit. It's useful when you want to take action on multiple separate audits that have no common aggregator or content provider by which to otherwise filter the search results.

Page Size: This function allows you to decide how many audits you'd like to view on a single page (e.g., show 100 audits per page).

Search: Don't forget to hit the Search button after selecting your search criteria! Search results will display in the main window below the search bar.

Other features of the Audit Search tab include customized sorting and exporting options. You can sort a column by clicking on the column heading. Links labeled Previous and Next, along with numbered links, allow you to navigate through results that span multiple pages. The Download as CSV link in the top-right corner of the search results window allows you to download the search results on the current page in a comma-separated values spreadsheet, which can be opened in Microsoft Excel.

CONTACTING THE CTIA SUPPORT TEAM

The CTIA Support Team is available to help all participants manage PSMS advertising and message flow compliance within the CTIA IMM Portal. Aggregators and content providers reach them on the Support Helpline at (855) 272-8182 or at support.ctia@psmsindustrymonitor.com for assistance with:

- Accessing program violation notices,
- Replying to audit notifications,
- Navigating the portal,
- Updating contact information, and
- Obtaining or resetting login credentials.

Enforcement specialists are standing by at the Support Desk to answer the helpline during normal business hours, from 9:00 A.M. to 5:00 P.M. EDST, Monday through Friday. They will help you understand how to correct your noncompliant advertisements and service messages so your audits can be closed.

When contacting the Support Desk via the email address, to help the Support Team handle queries and requests quickly and efficiently, please keep in mind the following:

- For questions regarding a specific audit, include the audit number in your email subject line.
- When requesting login credentials, include the associated audit number of the violation notice you're trying to access or the name of the content provider that received the notice.
 - Login credentials will be issued as official compliance contacts only to content provider email addresses registered in the CSC Registry, provided they match the company on file.
 - To be associated with a content provider's user name, the domain name of the email address must be associated clearly with the content provider name on file (e.g.,

audits@contentprovider.com). Email addresses from free email domains (e.g., howie@hotmail.com) are unacceptable as contacts for content providers and aggregators.

- When requesting technical assistance, attach screenshots of errors encountered and include a step-by-step description of the problem you're experiencing. The name of the browser you're using to access the portal also is useful information.

PROGRAM VIOLATION NOTICES

Program Violation Notices, known informally as *failure forms*, are PDF notifications of noncompliant advertising and message flows. The PSMS Industry Monitor ticketing system issues, to the responsible content providers and aggregators, violation notices every week via URL links in notification email. At the top of all violation notices are a unique audit number, the notice date and cure date, the program shortcode, and the names of the responsible content provider and aggregator or aggregators. Advertising notices include, in addition, the number of total interceptions of the ad and the number of total unique interceptions.

Each advertising violation notice displays a comprehensive list of violations committed on the associated shortcode and explains what the content provider must do to bring the advertisement into compliance with CTIA audit standards. Below the list of violations and actions required are thumbnail images of each unique piece of advertising creative intercepted on that shortcode and captured during the review period. For user convenience, unique creative are organized and numbered in groups with their duplicates. Therefore, the number of unique creative will correspond directly to the number of groups.

Click on any thumbnail to view an itemized list of the specific violations that apply to the individual unique creative and its related duplicates, with severity levels and actions required to correct the violations. Clicking on the thumbnail just above the itemized list will take you to a full-size screenshot or video clip of the creative as it appeared in market on the capture date. For online advertisements, the intercept location link will take you to the actual Website where the creative appears.

The links below the itemized list allow you to view related duplicate creative. In the event the unique creative is an affiliate marketer's advertisement, the links below the itemized list will take you, instead, to the content provider's advertisements, which are the pages linked to in the affiliate advertisement.

Message flow violation notices display the date and time the flow was initiated and a thumbnail image of an advertisement from which the message flow was generated. Subsequent pages in the violation notice contain copies of service messages intercepted by opting into the associated offer. Below each service message is an itemized list of violations committed in the message and the actions the carriers require to bring the message into compliance.

RESPONDING TO AUDITS THROUGH THE CTIA IMM PORTAL

Aggregators, carriers, and the CTIA can communicate directly through the CTIA IMM Portal.

1. Access the CTIA IMM Portal with your unique username and password.
2. Navigate to the relevant tab.
3. Search by selecting the appropriate audit status (e.g., Open, Pending Retest, Closed), shortcode, or audit number and clicking the Search button.

4. Refine your search further by selecting, for example, a specific severity in the Severity dropdown menu or a product type in the Products dropdown menu and clicking the Search button again. For more details, please see the list of search parameters in the Navigating the CTIA IMM Portal section on pages 1–3 of this User Guide.
5. Click the associated link in the Status column (i.e., Open, Pending Retest, Retest Failed, Escalated, Closed, or Withdrawn) when your search results appear, which will raise an email box.
6. Enter a message in the email box, if you wish, and view in the email chain other messages regarding this audit.

Aggregators, carriers, and the CTIA also can request a simple retest via the CTIA IMM Portal. Log into the portal, locate the program violation notice in the search results, and click on the Retest link in the Action column on the right side of the page. Clicking Retest automatically sends a template message to the CTIA Compliance Team, notifying them that the associated creative is ready for retest.

When submitting a message flow retest request by clicking Retest, aggregators must submit a corrected message flow copy at the same time via a portal email box. See numbers 5 and 6 above. The service messages should include the proposed corrections before they're made live. In this way, the Compliance Team can evaluate proposed corrections for compliance *before* the content provider incurs operational and time costs.

RESPONDING TO AUDITS VIA EMAIL

Content providers, aggregators, carriers, and the CTIA can request an audit retest by replying to the audit notification email, ***maintaining the original subject line***, and indicating that the associated creative or message flow is ready for retest. Email sent to this address without the correct subject line is discarded by the system, never reaching the CTIA Compliance Team. When submitting a message flow retest request, content providers or their aggregators must submit a corrected message flow copy at the same time. You may do so by attachment to the email or by entering the corrected copy in the body of the email. The service messages should include the proposed corrections before they're made live. In this way, the Compliance Team can evaluate proposed corrections for compliance *before* the content provider incurs operational and time costs.