

# TCPA Guardian Enhancements: Lead Seller Guidelines and Readiness Instructions

This document provides a detailed overview of the new TCPA Guardian enhancements to support the one-to-one consent requirements that go into effect on January 27, 2025. It includes the steps lead sellers must take to ensure their lead forms and flows are compatible, best practices and examples, an implementation checklist to ensure lead buyers receive accurate data responses from your forms and flows, and screenshots that show how TCPA Guardian clients will activate and manage the new one-to-one consent features.

## Table of Contents

How is the TCPA Consent Landscape Changing? .....	2
How is Verisk Marketing Solutions Evolving to Support the New 1:1 Consent Regulations? .....	2
What Do I Need to Do to Ensure My VMS Implementation is Ready for the Guardian Enhancements?.....	4
How Will My Lead Buyers Use TCPA Guardian?.....	7
Lead Seller Implementation Checklist .....	10
Examples of TCPA Guardian in Action .....	11
Sample API Responses and Descriptions .....	23

## How is the TCPA Consent Landscape Changing?

Per updated FCC regulations, brands that auto-dial using an Automatic Telephone Dialing System (ATDS), send text messages, or use prerecorded messages will need Prior Express Written consent from the consumer, and the consumer needs to explicitly opt-in to the individual companies that will be contacting them. Additionally, the calls that the consumer receives must be "logically and topically" associated with the content of the website where they requested to be contacted. These regulations go into effect January 27, 2025.

## How is Verisk Marketing Solutions Evolving to Support the New 1:1 Consent Regulations?

We are evolving our TCPA Guardian solution to enable lead buyers and sellers to meet the changing needs of FCC regulations. Below is an overview of how our Guardian solution works and how it's changing to support 1:1 consent.

### TCPA Guardian – How does it work?

- Lead generators implement the VMS script on their comparison-shopping websites, enabling VMS to be a neutral, 3rd party witnesser of a lead event and deliver reporting and calculations about the event.
- When a consumer lands on a page with the VMS script implemented, we issue a "LeadiD" that is specific to that lead event. The seller includes the specific LeadiD associated with the event when passing a lead to a buyer.
- When a LeadiD is presented to a buyer, the lead buyer makes a real-time API call to VMS to:
  - Gather real-time insights about the lead event to proactively determine whether a specific lead meets their compliance requirements. These real-time insights enable confident lead buying and treatment decisions.
  - Store visual proof of consumer consent to use as evidence in a TCPA complaint.
  - Lead generators also can also gain access to visual proof of consent on leads they generate, for their own risk mitigation solution.

## TCPA Guardian – How is it Evolving for the 1:1 Consent Regulations?

### Lead Funnels We Support

- **Exclusive Lead Flow**
  - Singular stand-alone brand-specific TCPA disclaimer
- **Shared Lead Flows**
  - General TCPA disclaimer text + brand names w/ individual check boxes
  - Dynamically Populated brand names within TCPA text + brand names with individual check boxes
  - Stand-alone brand-specific TCPA disclaimer text + brand names with individual check boxes
  - Multi-page matching with brand-specific TCPA disclaimer text on each page

### Product Evolution 1: Brand Name Consent

Lead buyers can verify that their approved brand name was presented to the consumer and selected by them in a manner they deem compliant. TCPA Guardian will capture consent within lead workflows that provide multiple brand opt-in options. We will be capturing consent for lead experiences involving static TCPA disclosures along with brand name checkboxes, as well as dynamic TCPA disclosures that update based on the user selections of the brand name checkboxes.

#### Brand Name Consent Functionality

##### (Publisher Implementation Instructions in Next Section)

- Lead buyers upload their approved Brand Name(s) in the [myJornaya](#) User Interface.
- Brand Names uploaded will be searched for during the lead event and insights will be returned in Guardian's real-time API response, determining if an exact match was found to any approved Brand Name. Buyers will know the specific Brand Names from their approved list that were witnessed at the lead event.
- For each Brand Name witnessed at the event with a checkbox, we will indicate if each Brand Name was or was not selected by the consumer, and how consent was provided (ex. Active / passive checkbox, etc.)
- For exclusive lead flows, lead buyers will make API calls using a separate "Audit Profile" (rule set in VMS' User Interface) to validate their singular brand was present in an approved TCPA disclaimer.
- Lead buyers can set real-time rules and see reporting for Brand Name and Consent verification.

## Product Evolution 2: Topical Relevance

Lead buyers will be able to confirm that the lead event purchased had topical relevance to the buyer's services being offered to the consumer. Ex.) Auto insurance carrier verifying if "auto insurance" was present in the lead funnel.

### Topical Relevance Functionality

#### (Publisher Implementation Instructions in Next Section)

- TCPA Guardian will verify that the content on the original website was topically relevant to the buyer, by adding a keyword search functionality.
- Lead Buyers upload their approved keywords in the [myJornaya](#) User Interface. These keywords will be searched in the webpage using labels.
- Buyers will know the specific Keywords from their approved list that were witnessed at the lead event.
  
- Lead buyers can set real-time rules and see reporting for Topical Relevance verification.

# What Do I Need to Do to Ensure My VMS Implementation is Ready for the Guardian Enhancements?

## Ensure You Have a Complete VMS Script Implementation

- Adding the VMS Script to your sites promotes trust and confidence with buyers as this shows a commitment to transparency and compliance. This also enables buyers to access data to make higher-performing conversion decisions once they purchase a lead.
- Ensuring a complete VMS Script implementation will help to avoid lead rejections for leads that could have passed your buyer's compliance criteria.
- Protect your own business – deploying the VMS script enables you to have a TCPA Guardian subscription of your own, to store and access visual proof of consumer opt-ins across your sites, to defend your business in the event of complaints.
- Expand your buyer network, as many lead buyers require LeadiDs to be delivered with any lead they purchase.

## Implement the VMS Script across lead funnels and on every page

(Including Thank-You Page / Post-Submissions)

### Why this is important

- Implementing the VMS script is a necessary step for TCPA Guardian to function, enabling buyers to validate compliant TCPA consent and for buyers + sellers to gather visual proof of consent.
- Implementing across the full website / funnel experience is critical to collecting full proof of consent.
- Implementing on a post-submission/ Thank-You page is critical to show proof that a consumer submitted their consent.

### How to implement

- Instructions Link: [Create Script Instructions](#)
- The VMS script functions to support a variety of different consent captures – checkboxes, submit buttons, radio buttons, and drop-down menus.

## Place TCPA labels around each specific TCPA disclosure

### Why this is important

- TCPA Labels are a critical step in the Implementation process – these labels direct our script to where to look for a TCPA disclosure, and therefore report insights that buyers rely on to determine compliance.
- Without TCPA labels, lead buyers cannot proactively determine a lead's compliance levels. Many lead buyers will reject these scenarios. Missing this step will result in lead rejections.

### How to implement

- Instructions Link: [How to Add Jornaya TCPA Label / Tags](#)
- The TCPA Disclosure label should be placed around the disclosure text displayed on your forms. We offer four different implementation options to support different user experiences:
  - No User Interaction Required (Consent given via form submission)
  - Checkbox
  - Radio Buttons
  - Yes/No Dropdown Menu

- Please refer to the implementation instructions to ensure you are following the correct instructions, based on how you are capturing consent for the TCPA disclosure.

## Place Label Tags and Input Checkboxes Around Brand Names

### **\*New Functionality\***

#### Why this is important

- Label/Input combinations are a critical step in the Brand Name Implementation process – these labels direct our script where to look for a brand name in the lead form and how to capture the consent provided by the consumer for each individual brand.
- This will help avoid lead rejections for compliance reasons.

#### How to implement

- [How to Add TCPA Brand Name Labels](#)
  - HTML instructions for lead forms and flows.
- [Setting Up Brand Names in myJornaya](#)
  - Instructions for adding brand names and rules in our UI.

## Ensuring Topical Relevance

### **\*New Functionality\***

#### Why this is important

- Lead buyers will be looking for topical relevance keywords that match their approved list, to ensure the web experience was consistent with their services being offered.
- This will help avoid lead rejections for compliance reasons.

#### How to implement

- [How to Set Up Topical Relevance in myJornaya](#)
- Ensure that the web pages that host lead forms contain keywords relevant to the requested consent.
- These keywords must exist on the page and in the HTML. We will not be verifying keywords within the TCPA disclosure text.

## Collect Your Lead Buyers' Approved TCPA Disclosures

### Why this is important

- To avoid lead rejections, ensure the TCPA disclaimers you're using exactly match the TCPA disclaimers that are approved and being used by your buyers. If they do not match, a buyer will receive a data response that an un-approved TCPA disclaimer was presented.

## Collect Your Lead Buyers' Approved List of Brand Names

### Why this is important

- We will be looking for an exact match between the brand name text displayed in your lead forms and flows and the official approved brand name list provided by the brand. You must use exact matches to avoid lead rejections for situations where a buyer receives a data response where they expect a brand name match and do not receive one.

## Understand How Your Buyers Will be Using TCPA Guardian Responses to Mitigate Compliance Risk

### Why this is important

- Alignment with your buyers on their specific rules they will be using to make decisions will help proactively avoid lead rejections for non-compliance, and help you act as an extension of your lead buyers' teams

## How Will My Lead Buyers Use TCPA Guardian?

### To Make Real-Time Decisions for TCPA Risk Mitigation

- Lead buyers accessing TCPA Guardian use a variety of real-time data responses to make real-time decisions before they accept a lead. Buyers will use Guardian's real-time responses to determine each lead's compliance status (relative to their specific compliance standards) and make real-time decisions such as if they will accept a lead or how they will communicate with a lead (ex. dial vs. email).

- Real-time decision logic is specific to each lead buyer. Each lead buyer may have their own specific compliance ruleset with VMS' User Interface, and each buyer may use various TCPA Guardian real-time responses in their own specific way.
- E.g., Buyer A may have pass/fail requirements for every Guardian data response and reject leads with any failures. Buyer B may have pass/fail requirements for every Guardian data response, and but only reject leads with Disclosure, Brand Name, and Consents Failures (and use other failure responses to determine if they will dial vs email).

## To Provide Real-Time Data Responses to Lead Buyers to Assess Compliance

- Did VMS witness a tagged TCPA Disclosure at the original lead event?
- Did the TCPA Disclosure witnessed match a disclosure in the buyer's approved list?
- What type of consent was provided for the TCPA disclosure?
- Checkbox, radio button, drop-down menu, no interaction required
- What action did the consumer take?
- For checkboxes, radio buttons or Yes/No drop down - Active Consent, Passive Consent, Active Decline, Passive Decline
- Consent No interaction required
- What was the font size of the disclosure?
- What was the contrast in color between disclosure text color and page background color?
- What was the overall visibility of a disclosure?
- Did VMS capture a Visual Playback?
- Did VMS store a Visual Playback?
- New Data Response
  - Which of the buyer's approved brand names were and were not witnessed at the lead event?
  - Which of the buyer's approved brand names were and were not selected by the consumer?
  - How did the consumer select the buyer's witnessed brand name(s)?
  - Which of the buyer's topical relevance keywords were and were not witnessed at the lead event?

## To Defend Against Complaints

- TCPA Guardian clients (Lead Sellers and Lead Buyers) use Compliance Reports and Visual Playbacks (visual re-renderings of the lead event) to show visual evidence of how the consumer consented at the lead event to defend complaints that arise.
- Lead buyers use Guardian's real-time responses to proactively avoid leads that do not meet their compliance criteria. This also enables them to be confident that when a



complaint arises, the Compliance Report and Visual Playback will show an opt-in experience that is consistent with their compliance requirements.

## For Ongoing, Detailed Compliance Tracking Across Affiliates

- Lead buyers using TCPA Guardian access BI dashboards and ongoing reporting to maintain a consistent understanding of compliance rates across their affiliates, to identify any issues and track fixes.

## Lead Seller Implementation Checklist

### VMS Script

- Script is implemented across every page of every funnel, including thank-you / post-submission page
- Every TCPA disclaimer is properly tagged with VMS' TCPA labels
- VMS LeadiDs are being created and stored with every session
- VMS LeadiDs are being passed with lead posts to buyers

### Brand Names

- Exact approved brand names have been collected from buyers
- Each brand name is placed within VMS' brand label tag in the HTML
- Each brand name includes an associated checkbox and is inside a label tag

### TCPA Disclaimer Language

- Coordinate with lead buyers on the exact approved TCPA disclaimer language(s) that will be used and accepted. Ensure all languages in-use are:
  - Approved by specific buyer
  - Uploaded to lead buyers' list of approved TCPA languages in their VMS rulesets – your lead buyers will be responsible for this piece.

### Topical Relevance

- Exact approved Topical Relevance keywords have been collected from buyers
- Necessary Topical Relevance keywords are shown in funnel.

### How Your Buyers use Guardian Responses in Real-Time.

- Have met with buyer's and thoroughly understand how they will be using TCPA Guardian responses to mitigate compliance risk

### Compliance Across Affiliate-Generated Volume

- If you are also buying leads to supplement leads generated on your owned and operated properties and want to proactively understand each lead's compliance level before purchasing, connect with Verisk Marketing Solutions to learn more details about accessing TCPA Guardian.

## Examples of TCPA Guardian in Action

### Lead Buyer Ruleset in the User Interface

How lead buyers will set up brand names.

#### Brand/Seller Names ✕

Enter the specific brand/seller names that you want to confirm are present on the lead form. If a match is found on the lead event, the audit response will return the brand name and consent status of the matching brand name.

Example 1:  
brand name1 | brand name2 | brand name3

Example 2:  
brand name1  
brand name2  
brand name3

Delimiter: Pipe (|) or a newline

save cancel







How lead buyers will set up rules/flags for brand names.

### Brand Names/Sellers

The TCPA compliance application allows you to set business rules around the specific form of consent that the user provided in association with the specified brand name(s) in the lead form.
















#### Brand Name Present

Allows you to verify if a specified brand/seller name matched with what was present on the lead form or not.

Brand Name present	 Pass	 Review	 Reject
Brand Name not present	 Pass	 Review	 Reject

#### Brand Name consent

Allows you to verify if a checkbox was present next to the brand/seller name in the lead form.

Brand Name no consent Checkbox was not present for the brand name to give consent to	 Pass	 Review	 Reject
Brand Name actively accepted Consumer proactively selected checkbox option for brand name	 Pass	 Review	 Reject
Brand Name passively accepted Checkbox associated with brand name was pre-populated for the user	 Pass	 Review	 Reject
Brand Name passively declined Consumer did not provide consent and checkbox option was not pre-populated	 Pass	 Review	 Reject
Brand Name actively declined Consumer proactively deselected checkbox for brand name	 Pass	 Review	 Reject

How lead buyers will set up topical relevance keywords.

### Topical Relevance ✕

Enter the specific keywords that you want to confirm are present on the lead form in order to make sure the webpage has relevance to the service being offered. If a match of a keyword is found on the lead event, the audit response will return the keyword(s) and whether they were present or not on the website.

Example: insurance, mortgage, car loans...







Delimiter: Comma (,) or Pipe (|)

save cancel

How lead buyers will set up topical relevance keywords.

### Topical Relevance

The TCPA compliance application allows you to set business rules around the specific keywords your organization has requested to be present on the lead form in order to validate topical relevance. If a match of a keyword is found on the lead event, the audit response will return the keyword(s) and whether they were present or not on the website.

Keyword(s) present	 Pass	 Review	 Reject
Keyword(s) not present	 Pass	 Review	 Reject

How lead buyers will upload their approved TCPA disclosures.

### Disclosure Text ✕

Enter the specific TCPA disclosure that you would like to confirm is present on the lead form.  
If a match is found on the lead event, the audit response will return the text of the matching disclosure. Do not enter any HTML tags in the disclosure.  
You may also check for specific phrases instead of a full disclosure by entering pipe (|) separated phrases in the disclosure box. Note that the successful response will only be returned if ALL pipe separated phrases are present in the disclosure found during the lead event.  
For example: first part of disclosure | my brand name | remainder of disclosure

---

### Vendor

Vendor Name

Select Vendor

---

### Notes

Notes










Disclosure Type: 3rd Party

How lead buyers will set up rules / flags for additional responses.

### TCPA Disclosures

#### Specified TCPA Disclosure

The TCPA compliance application allows you to set business rules around the specific TCPA disclosure your organization has requested be present on the lead form.

<b>Disclosure Match</b> A matching TCPA disclosure was present on the lead form	 Pass	 Review	 Reject
<b>Disclosure Mismatch</b> The disclosure found on the form does not match a specified TCPA disclosure	 Pass	 Review	 Reject
<b>Disclosure Absent</b> Cannot confirm that a specified TCPA disclosure was present during the lead event	 Pass	 Review	 Reject
















save cancel



## Consumer's Consent

### Consumer's Consent

The TCPA compliance application allows you to set business rules around the specific form of consent that the user provided in association with the specified TCPA disclosure.













<b>Consent actively provided</b> Consumer proactively selected consent option	 Pass	 Review	 Reject
<b>Consent passively provided</b> Consent was pre-populated for the user	 Pass	 Review	 Reject
<b>Consent passively declined</b> Consumer did not provide consent and consent option was not pre-populated	 Pass	 Review	 Reject
<b>Consent actively declined</b> Consumer proactively deselected consent option	 Pass	 Review	 Reject
<b>No interaction required on the form</b> Consent was given via form submission	 Pass	 Review	 Reject

save cancel

## TCPA Consent Type

### TCPA Consent Type

Provides the type of TCPA consent input present on the form
















Checkbox	 Pass	 Review	 Reject
Radio Button	 Pass	 Review	 Reject
Yes/No Dropdown Menu	 Pass	 Review	 Reject
No user interaction required	 Pass	 Review	 Reject

save cancel

## Prominence

### Prominence

The TCPA compliance application allows you to set flags based on the font size of the text of the express consent
















<b>Font size is 12pt or greater</b> Disclosure font size is at least 16px (12pt)	 Pass	 Review	 Reject
<b>Font size is between 6.75pt and 12pt</b> Disclosure font size is between 9 and 15px (6.75pt - 11pt)	 Pass	 Review	 Reject
<b>Font size is less than 6.75pt</b> Disclosure font size < 9px (less than 6.75pt)	 Pass	 Review	 Reject
<b>Font Size Unavailable</b> Disclosure font size is unavailable	 Pass	 Review	 Reject
<b>Hidden</b> The Specified TCPA disclosure was not visible during the lead event	 Pass	 Review	 Reject

save cancel

## Contrast

### Contrast

The TCPA compliance application allows you to set flags based on the contrast between the font color of the disclosure text and the color of the background on which the text was presented
















<b>Contrast is greater than 40%</b> There is at least a 40% contrast between the text color and the background color	 Pass	 Review	 Reject
<b>Contrast is between 25% and 40%</b> There is at least a 25% contrast between the text color and the background color	 Pass	 Review	 Reject
<b>Contrast is below 25%</b> The contrast between the text color and the background color is lower than 25%	 Pass	 Review	 Reject
<b>Contrast is unavailable</b> The contrast between the text color and the background color is unavailable	 Pass	 Review	 Reject
<b>Hidden</b> The Specified TCPA disclosure was not visible during the lead event	 Pass	 Review	 Reject

save cancel

### Composite Visibility

#### Composite Visibility

The TCPA compliance application allows you to set flags based on the composite score of the prominence and contrast scores










<b>Overall visibility is high</b> The composite visibility score is greater than 50	 Pass	 Review	 Reject
<b>Overall visibility is medium</b> The composite visibility score is between 20 and 50	 Pass	 Review	 Reject
<b>Overall visibility is low</b> The composite visibility score is less than 20	 Pass	 Review	 Reject
<b>Overall visibility is unknown</b> The visibility of the disclosure is unknown, or if there is not a TCPA disclosure match	 Pass	 Review	 Reject
<b>Hidden</b> The Specified TCPA disclosure was not visible during the lead event	 Pass	 Review	 Reject

save cancel

### Visual Playback Capture Verification

#### Visual Playback Capture Verification

Verifies that the Visual Playback has been captured.







<b>Captured</b> The Visual Playback of the lead event was fully captured	 Pass	 Review	 Reject
<b>Partially Captured</b> The Visual Playback of the lead event was partially captured	 Pass	 Review	 Reject
<b>Not Captured</b> The Visual Playback of the lead event was not captured	 Pass	 Review	 Reject

save cancel

### Visual Playback Storage Verification

#### Visual Playback Storage Verification

Verifies that the Visual Playback has been stored.

<b>Stored</b> The Visual Playback of the lead event was stored	 Pass	 Review	 Reject
<b>Not Stored</b> The Visual Playback of the lead event was not stored	 Pass	 Review	 Reject

save cancel

# Sample API Responses and Descriptions

## Brand Name Fields and Values

Brand Name		
Data Point	Value	Description
brand_name	{string}	Brand name #1 present during the lead event.

Brand Name Present		
Data Point	Value	Description
brand_name_present	0	The specified brand was not present in the lead form
	1	A matching brand name was present on the lead form.

Brand Name Consent		
Data Point	Value	Description
brand_name_consent	0	The brand name was not present and/or a checkbox is <b>not</b> present for this brand name
	1	Active Consent - The consumer proactively selected the checkbox next to the brand name
	2	Passive Consent - Checkbox was pre-populated for the user.
	3	Passive Decline - The consumer <b>did not</b> provide consent, and the checkbox was not pre-populated.
	4	Active Decline - The consumer proactively deselected the checkbox next to the brand name.
brand_name_consent_rule	#	Returned flag color for 'disclosure': 1 - 'Green'; 2 - 'Yellow'; 3 - 'Red'

## Brand Name API Response

```
"brand_names": [  
  {  
    "brand_name": "brand name 1",  
    "brand_name_present": 1,  
    "brand_name_present_rule": 1,  
    "brand_name_consent": 1,  
    "brand_name_consent_rule": 1,  
  },  
  "brand_name": "BRAND name 2",  
  "brand_name_present": 1,  
  "brand_name_present_rule": 1,  
  "brand_name_consent": 1,  
  "brand_name_consent_rule": 1,  
},  
  "brand_name": "Brand name 3",  
  "brand_name_present": 1,  
  "brand_name_present_rule": 1,  
  "brand_name_consent": 2,  
  "brand_name_consent_rule": 2,  
},  
},
```



## Topical Relevance Fields and Values

Topical Relevance		
Data Point	Value	Description
keyword	{string}	Keyword present during the lead event in the webpage.
keyword_present	0	Keyword(s) does not match a specified keyword in the audit profile.
	1	A matching keyword(s) was present on the lead form.

## Topical Relevance API Response

```
"topical_relevance": [
  {
    "keyword": "insurance",
    "keyword_present": 1
    "keyword_present_rule": 1
  },
  {
    "keyword": "mortgage",
    "keyword_present": 1
    "keyword_present_rule": 1
  }
],
"result": 2
```