



Campaign Verify



Campaign Verify is a **secure, non-partisan, nonprofit verification solution for U.S. political actors seeking to verify their identity and engage with voters via text messaging.**

Most major digital platforms, such as Facebook and Google, have created policies and protocols to verify U.S. political actors seeking to communicate with voters on their own platforms. **Campaign Verify hosts the analogous process for SMS messaging.**

Campaign Verify aims to **prevent spoofing and disinformation in political messaging** by acting as the verification layer for campaigns, committees, and PACs. CV serves the wider 10DLC ecosystem as the political vetting partner for [The Campaign Registry](#).

How does it work?

Campaign Verify:

- **Validates that campaigns are in fact who they say they are**
- **Creates authentication tokens which signal to The Campaign Registry, carriers, and service providers that they have been verified**

By requiring campaigns to have a verification token, Campaign Verify aims to prevent bad actors from spoofing a campaign and increase trust in the messaging ecosystem.

Verification costs \$95 per verification request per 2-year election cycle. All tokens issued in 2021 and 2022 will be valid through January 31, 2023.

Who is eligible for CV verification?

- **Any campaign, committee, or PAC registered with FEC**
- **Any State, Local, or Tribal candidate or committee registered with an election authority**

Federal campaigns and organizations registered with the FEC are required to submit their FEC ID, along with their campaign address and contact information.

State, Local, and Tribal campaigns submit a URL from their election authority that contains their filing record, which must contain at least one of the following: a postal address, email address, or phone number.

How does verification work?

After submission, a Campaign Verify staffer examines the verification request. Approval (or feedback on a Rejection) will take no more than two business days.

Once approved, a PIN will be sent via email, text, phone call or postal mail to the contact information listed on their filing record.

Once they receive a PIN code, they log into Campaign Verify using the same email account they used to send the submission, and enter the PIN code.

After the correct PIN code has been entered, the submission has been verified. They can now generate a secret Authorization Token to send to their texting provider, which can be submitted to The Campaign Registry to unlock special Political 10DLC campaigns and throughputs.

What do I need to do as a CSP?

If you are a CSP that integrates with The Campaign Registry either directly or via another platform provider that applies for TCR registration on your behalf, you simply need to collect CV tokens from your customers and submit them via The Campaign Registry API, or portal of TCR, or your platform provider along with any other Brand information you collect.

If you would like, you can get an API token from Campaign Verify that lets you check the validity of CV tokens submitted to you. This may be helpful to catch issues with tokens before you submit them to TCR or your provider, as well as help protect you from potentially fraudulent users.

API documentation and a token verification portal is available for CSPs that would like to check tokens themselves to validate them before submission to TCR.



How does a CSP get access to the API?

- Send an email to serviceproviders@campaignverify.org to request API access
- Campaign Verify will send an API data contract for signature via DocuSign (this is free of charge for all CSPs)
- Once signed, Campaign Verify staff will send API documentation, a Test API Key and test tokens, as well as a live API key to validate your users' tokens

Can this process be automated?

The key to secure verification is in the submission of the PIN code to the email address, phone number, or mailing address on a public filing document, so there is a limit on what can be automated. Campaign Verify provides the ability to submit multiple verification requests from a single account. However, there is no API to submit verification requests. The API can only be used for checking tokens.

Campaign Verify encourages CSPs to ask their customers to get verified by Campaign Verify themselves, rather than apply on their customers' behalf.

In the verification process, the PIN correspondence contains the name of the person who submitted the request (tied to a Campaign Verify account). This is to help guide the manager of inboxes listed on filing forms, who may be on the compliance team and not familiar with Campaign Verify when they receive the PIN. To prevent spoofing and phishing, they should be familiar with the individual requesting the verification, as opposed to the name of an employee of a vendor.

What resources can I give to my customers?

You can direct your customers to go to <https://www.campaignverify.org>, read the information, and submit their information in the form. A FAQ is available [here](#).

Once they enter the information, they will receive an email with a link to <https://app.campaignverify.org> where they can create a Campaign Verify account via email signup.

Once they sign up, they can request a new verification via the New Verification Request button.



+ New Verification Request

After submission and payment, they will receive an email when the request has been approved or rejected. If approved, an email, text, call or letter with their PIN code will go to the relevant contact information on their filing form. Campaign Verify may also contact the requester for more information prior to approval or rejection.

How should I collect tokens from my customers?

Campaign Verify tokens are secure identifiers and should be treated as such, similar to API keys or other secrets.

You should collect them via a secure process, such as a web form using https, and store them in a secured database.

If you believe that a CV token from one of your customers has leaked, please contact serviceproviders@campaignverify.org.

What is the policy around re-use of a CV token?

CV TCR tokens are meant to be scoped to a single TCR Brand, and not reused across multiple Brands.

If there are multiple ISVs or consultants working with the committee, they should request a new Authorization Token for each TCR Brand that will be registered.

What is the format of a CV token?

A full CV token is comprised of 6 pipe (|) delimited fields For example:

```
cv|1.0|tcr|10dlc|9957c339-d46f-49b7-a399-2e6d5ebac66d|GQ3NMEjED8xSlaAgR  
XAXXBUNBT2AgL-LdQuPveFhEyy
```

1. CV prefix: this will always be “cv”
2. Token version: currently 1.0
3. Service ID: For tokens consumed by the Campaign Registry, this will be “tcr”
4. Channel ID: For 10DLC tokens, this will be “10dlc”
5. CV Committee ID: UUID
6. Secret: 32 bit URL safe random string

FAQ

- Please see the [FAQ here](#)
- If you would like to get a CV API key, please reach out to serviceproviders@campaignverify.org
- For all other questions, please reach out to serviceproviders@campaignverify.org
- Thank you!