



BETTER MESSAGING

campaign registry

Authentication+

Product/Technical Specifications Document

Updated November 28, 2024

Changes in this document update:

- Added information on changes to external vetting, additional FAQ with tips on how to get 2FA verification completed quickly, and how to troubleshoot 2FA errors.

Note: Changes from the previous version of this document are **highlighted in yellow**.



Table of Contents

Summary	4
Brand Attestation	4
Additional Brand Information Capture	4
New Public Profit Entity Type Brand Registration.....	5
Updates to Legacy Public Profit Entity Type Brands.....	6
Authentication+ Business Rules	7
Brand Identity State and Transitions	8
Brand Initial States.....	8
New Public Profit Brands.....	8
Legacy Public Profit Brands.....	9
VERIFIED State (After Authentication+).....	9
VETTED_VERIFIED State (After Authentication+).....	10
Multiple 2FA Emails	10
Impacted CSP API Endpoints	11
Existing Endpoints.....	11
New Endpoints.....	17
Impacted DCA API Endpoints	18
Existing Endpoints.....	18
Impacted MNO API Endpoints	19
Existing Endpoints.....	19
2FA Notification Events	20
FAQ	21



BETTER MESSAGING

campaign registry

Document History

Date	Comment	Author
4/18/2024	Initial publication.	Saransh Srivastava
6/27/2024	Updated the FAQ section with additional information about legacy campaigns.	Saransh Srivastava
8/8/2024	Updated validation rules, FAQ, and information about sending multiple 2FA emails. Adjusted document formatting for readability.	Victor Cardoso
8/22/2024	Added information on the Auth+ 2FA Verification Flow for new and legacy brands, and pricing information in the FAQ.	Victor Cardoso
9/5/2024	Updated some document wording and added new questions to the FAQ section.	Victor Cardoso
9/19/2024	Added a new release date, new questions to the FAQ section, and additional details on API responses.	Victor Cardoso
10/3/2024	Updated the FAQ section and added additional details about new and existing Public Profit brands in their initial states.	Victor Cardoso
10/17/2024	Updated the format of the businessContactEmail VerifiedDate attribute. Also added more information about initial pricing, the initial identity status returned by the CSP API, and what the Pending label means in the CSP portal.	Victor Cardoso
10/31/2024	Added new questions to the FAQ along with information that the Website/Online Presence field will be required for Public Profit brands in Q2 of 2025.	Victor Cardoso
11/14/2024	Added more information on the process of registering and resubmitting Public Profit brands.	Victor Cardoso
11/28/2024	Added information on changes to external vetting, additional FAQ with tips on how to get 2FA verification completed quickly, and how to troubleshoot 2FA errors.	Victor Cardoso



BETTER MESSAGING

campaign registry

Summary

Authentication+ is TCR's new brand identity verification process for Public Profit brands available in release 5.20. The primary objective is to prevent brand impersonation, which leads to consumer fraud such as disinformation, smishing, and spoofing. This new brand identity verification process requires brand personnel attestation via Two-Factor Authentication (2FA) as part of the initial brand registration flow. Initially, Authentication+ is mandatory and only applicable to brands with a Public Profit entity type. In future releases, support for other entity types will be added. Authentication+ also lays the foundation for RCS support in TCR, and brands that complete the verification process will also meet brand verification requirements for RCS.

Brand Attestation

Many industry entities have expressed the need to incorporate more checks in the brand verification process to prevent brand impersonation. As part of Authentication+, Public Profit brands are now required to complete a new 2FA/brand attestation step during the brand registration process. Upon successful completion of the 2FA, the said brand's identity status will be marked as VERIFIED and allowed to create 10DLC campaigns.

Additional Brand Information Capture

To complete Authentication+ brand attestation, CSPs are required to submit the email address of a business contact who works at the brand and who can complete the 2FA.

A new field called Brand Contact Email is required during the brand registration flow on the CSP portal, and a new mandatory `businessContactEmail` parameter when using the brand registration API. This enables CSPs to enter a brand contact email address as part of registration.

Note: *In Q2 of 2025, the Website/Online Presence field will be required for Public Profit brands. This field is an important component of Authentication+ verification.*



BETTER MESSAGING

campaign registry

Upfront Validation of Brand's Business Contact Email ID Field

TCR will perform an upfront validation of the brand's business email address. TCR will reject email addresses that match the following conditions:

- Non-well-formed email addresses
- Personal and free email addresses
- Common email distribution addresses

If a brand fails any of the above validation rules, the brand registration request will be rejected. CSPs will need to re-submit the brand information with a valid brand email address.

New Public Profit Entity Type Brand Registration

For new brands with a Public Profit entity type, CSPs will submit the email address of a brand business contact as part of the Authentication+ brand registration flow. If the email address passes TCR's initial validation (e.g., a well-formed email address, not a personal or free email address, or not a common email distribution address), then the brand identity verification process will be initiated.

Brand Identity Verification Flow

As part of brand identity verification, TCR performs a basic identity verification (matching the EIN/Tax ID with the legal entity name). Next, TCR verifies whether the business email address is associated with the brand. Once the association is established, a 2FA email is sent to the brand's business contact.

If either the basic identity verification or the email association check fails, the 2FA will not be triggered and the brand will change to an UNVERIFIED identity status.

2FA Verification Flow

The 2FA email will contain a Verification PIN and a link. When the brand contact clicks on the link, they will be directed to a site and be prompted to enter the following information:

- Brand Contact First Name
- Brand Contact Last Name
- Brand Contact Job Title
- Verification PIN from the 2FA email

The brand contact will then click a **Complete** button to submit the information. Once the 2FA is complete, the brand will transition to a VERIFIED state and CSPs will be able to register campaigns.



BETTER MESSAGING

campaign registry

Resending a 2FA Email Link

If the 2FA email link is not clicked within 7 days of delivery, CSPs can resend the email up to 30 days from the initial request. If 30 days pass from the initial request and the 2FA verification process has not been completed, the CSP will need to resubmit the brand.

Updates to Legacy Public Profit Entity Type Brands

Legacy brands that are in a VERIFIED or VETTED_VERIFIED state will need to be Authentication+ compliant to register new campaigns. Active campaigns associated with a Public Profit entity type brands are not immediately impacted. However, CSPs will not be able to add new campaigns until they update the brand's business contact email. Once updated, the brand will transition into an UNVERIFIED state and the CSP will need to resubmit the brand.

Upon resubmission, the brand will undergo the same identity verification process as new brands (see the Brand Identity Verification Flow above). A 2FA email will then be sent to the brand business contact and they will need to complete the same process as specified in the 2FA Verification Flow (clicking a link, entering information, and clicking Complete).

For the initial rollout, TCR will refund the cost to revert existing Public Profit brands with a VERIFIED or VETTED_VERIFIED identity status that choose to go through Authentication+ verification. The revert fee will not be applied, so it will not appear on the billing invoice.

Upon successful completion of the 2FA process, the brand will be restored to its previous status of VERIFIED or VETTED_VERIFIED provided there have been no other changes to the identity fields (Brand Entity Type, EIN, EIN Issuing Country, or Company Name). If 2FA verification fails, the brand will remain in an UNVERIFIED status.



BETTER MESSAGING

campaign registry

Authentication+ Business Rules

- New Public Profit brands will not be VERIFIED nor qualify for a new campaign until the brand's contact email is added and 2FA confirmed.
- Already registered (Legacy) Public Profit entity type brands do not qualify for new campaigns until the brand business contact email is updated by the CSP and is 2FA confirmed.
- Active campaigns associated with Public Profit entity type brands are not immediately impacted by the Authentication+ rollout. However, as per MNO regulations, all Public Profit brands will eventually need to be brought to Authentication+ compliance at a future date. This will be communicated in a future documentation update.
- When a brand's business contact email field is updated for Public Profit brands in a VERIFIED/VETTED_VERIFIED identity status, the identity status will revert to UNVERIFIED. While in the UNVERIFIED status:
 - The brand does not qualify for new campaigns.
 - The brand does not qualify for an external vet.
 - Existing active campaigns will remain active and not be affected.
 - Existing external vets are not applicable to the brand until the brand is 2FA verified.
 - The CSP will need to resubmit the brand to initiate the 2FA process. The brand identity status will be restored when the brand is 2FA confirmed, provided there have been no other changes in the following identity fields: Brand Entity Type, EIN, EIN Issuing Country, Company Name.



Brand Identity State and Transitions

Brand Initial States

Each of the following initial Public Profit brand states **will not qualify for a new campaign** until the brand's business contact email address is added and the brand is submitted (or resubmitted) for Authentication+ compliance:

- A new brand
- A legacy brand in an UNVERIFIED state
- A legacy brand in a VERIFIED state (with or without campaigns)
- A legacy brand in a VETTED_VERIFIED state (with or without campaigns)

New Public Profit Brands

When a new Public Profit brand is submitted via the portal or API, the brand will not attain any identity status until the Authentication+ process is complete. In the CSP portal, its identity status will be shown as *Pending*. In the CSP API, the brand's `identityStatus` attribute will be empty or return null. A brand will not attain a valid identity status until the brand's business contact responds to the 2FA email.

If the brand does not respond within 7 days, the 2FA will expire. The CSP can send a new 2FA email to the brand within 30 days of the brand's initial registration. After 30 days, if the brand has still not responded, the identity status will change to UNVERIFIED and it will need to be resubmitted to trigger a new 2FA email.

Transitions to UNVERIFIED State

If the Authentication+ process fails, then the brand transitions to an UNVERIFIED state. There are several potential reasons for failure. Some of these include:

- An identity check failure due to bad or mismatched identity fields (e.g., the EIN doesn't correspond to the company name).
- Inconclusive or insufficient evidence to substantiate the relationship between the brand's business contact email and the brand (e.g., the email domain is not connected to or does not belong to the business).

The reasons for the failure are available to the CSP via the existing feedback loop mechanism.



BETTER MESSAGING

campaign registry

Transitions to VERIFIED State

If the Authentication+ process is successful, then the brand transitions to a VERIFIED state. At this point, the brand can qualify for a new campaign.

Legacy Public Profit Brands

Legacy Public Profit brands will remain in their current state until they update their brand business contact email address. Once they add this information, they will transition to an UNVERIFIED state. The brand will then need to be resubmitted, which triggers the Authentication+ verification process. Legacy public profit brands will not be able to register new campaigns until they become Authentication+ verified.

Transitions to VERIFIED State

If the Authentication+ process is successful, then the brand transitions to a VERIFIED state. At this point, the brand can qualify for new campaigns.

Transitions to VETTED_VERIFIED State

If the Authentication+ process is successful and there is a valid existing external vet for the brand, the brand transitions to a VETTED_VERIFIED state. This transition is only possible for legacy brands in a VETTED_VERIFIED identity status after updating their business contact email and completing the 2FA email verification.

VERIFIED State (After Authentication+)

This is an Authentication+ compliant state where the brand is eligible to register new campaigns.

Transitions to UNVERIFIED State

If any of the Authentication+ fields (Entity Type, EIN, EIN Issuing Country, Company Name, Business Contact Email Address) is changed, the brand will transition to an UNVERIFIED status. However, note that modification of identity fields (Entity Type, EIN, EIN Issuing Country, Company Name) is not allowed for brands with an active campaign or an active external vet.



BETTER MESSAGING

campaign registry

Transitions to VETTED_VERIFIED State

A brand in a VERIFIED identity state is eligible for an external vet. A successful external vet will upgrade the brand identity state to VETTED_VERIFIED.

VETTED_VERIFIED State (After Authentication+)

This is an Authentication+ compliant state with an external vet. The brand is eligible to register new campaigns at a potentially higher throughput than the VERIFIED state for some MNO networks.

Transitions to UNVERIFIED State

If any of the Authentication+ fields (Entity Type, EIN, EIN Issuing Country, Company Name, Business Contact Email Address) is changed, the brand will transition to the UNVERIFIED state. However, note that modification of identity fields (Entity Type, EIN, EIN Issuing Country, Company Name) is not allowed for brands with an active campaign, active external vet, or pending appeal requests.

Multiple 2FA Emails

If a brand is registered with more than one CSP, it's possible that multiple 2FA emails will be sent to the same brand contact. This situation can result in a damaged domain reputation and 2FA emails being marked as spam or the TCR email domain being blacklisted by email servers.

To prevent this, TCR will only send one 2FA email to the brand business contact address within a two hour window. This rule will apply to all CSP actions that trigger a 2FA email, including brand registration, brand revet, and requesting a resend of a 2FA email.



Impacted CSP API Endpoints

Existing Endpoints

Register Brand

POST /brand/nonBlocking

A CSP is expected to use the same API endpoint to register Public Profit entity type brands. This endpoint has a new **mandatory** field: **businessContactEmail** which is applicable when the brand entity type is PUBLIC_PROFIT.

This endpoint will perform upfront validation of the **businessContactEmail** field, comprised of the following rules:

- Reject non-well-formed email addresses
- Reject personal and free email addresses
- Reject common email distribution addresses

If a brand fails on any of the above validation rules, the brand registration request is rejected with error code 553. Upon passing validation, the brand is submitted to Aegis's Authentication+ endpoint for Public Profit entity type organizations.

Required Fields

Field name	Type	Length	Description
businessContactEmail	String	100	Brand's business contact email address. Note: Free or personal email addresses are not supported.

Error Codes

TCR Error Code	Fields	Description
553	businessContactEmail	Unsupported email address.



Update Brand

PUT /brand/{brandId}

A CSP can use this API endpoint to update the **businessContactEmail** field for Public Profit entity type brands. If the **businessContactEmail** is changed and not null, then it must pass the following set of validation rules:

- Reject non-well-formed email addresses
- Reject personal and free email addresses
- Reject common email distribution addresses

If a brand fails on any of the above validation rules, the brand registration request is rejected with error code 553.

Points to note:

- Updating the **businessContactEmail** field will cause the brand identity status to become UNVERIFIED. This rule applies to brands with and without campaigns. This rule also applies to brands in VERIFIED and VETTED_VERIFIED statuses.
- Legacy brands that lost the VETTED_VERIFIED status as result of an update to the **businessContactEmail** field can regain the VETTED_VERIFIED status upon completion of the Authentication+ process. There is no need to reapply or re-import an external vet.

Error Codes

TCR Error Code	Fields	Description
553	businessContactEmail	Unsupported email ID.



New External Vet

POST /brand/{brandId}/externalVetting

Public Profit entity type brands in an UNVERIFIED state will no longer be eligible for vetting to directly upgrade to a VETTED_VERIFIED state. **Note:** *Public Profit entity type brands must be in either a VERIFIED or VETTED_VERIFIED status to qualify for new vetting.*

Error Codes

TCR Error Code	Description
525	External vet not supported for a brand in an UNVERIFIED identity status.

Import External Vet

PUT /brand/{brandId}/externalVetting

Public Profit entity type brands in an UNVERIFIED status will no longer be eligible to import vetting to directly upgrade to the VETTED_VERIFIED state. **Note:** *Public Profit entity type brands must be in either a VERIFIED or VETTED_VERIFIED state to import an external vet.*

Error Codes

TCR Error Code	Description
525	External vet not supported for brand in an UNVERIFIED identity status.



BETTER MESSAGING

campaign registry

Get Brand Info by Brand ID

GET /brand/{brandId}

Public Profit entity type brands in a VERIFIED or VETTED_VERIFIED status will return new fields in the response.

New Fields

Field name	Type	Length	Description
<code>businessContactEmail</code>	String	100	Brand's business contact email address. Note: Free or personal email addresses are not supported.
<code>businessContactEmailVerifiedDate</code>	String	N/A	An ISO 8601-formatted date and time of the successful 2FA email completion.

Search Brands

GET /brand

This endpoint now supports a new filter:

- **authenticationPlusCompliant:** This filter returns brands whose `businessContactEmailVerifiedDate` is not null.

Public Profit entity type brands in a VERIFIED or VETTED_VERIFIED status will return new fields in the response.

New Fields

Field name	Type	Length	Description
<code>businessContactEmail</code>	String	100	Brand's business contact email address. Note: Free or personal email addresses are not supported.
<code>businessContactEmailVerifiedDate</code>	String	N/A	An ISO 8601-formatted date and time of the successful 2FA email completion.



Get Brand Feedback

GET /brand/feedback/{brandId}

This endpoint will return a new category called WEB_DOMAIN. The response will include details in the **errors** attribute with more information as to the specific nature of the problem.

New Category

Field name	Description
WEB_DOMAIN	Not valid/recognised email domain.

Error Codes

Field name	Description
TFWD01	The submitted business contact email is not an allowable domain.
TFWD02	The submitted business contact email domain ownership cannot be independently verified.
TFWD03	The PIN issued on the submitted business contact email has expired without a response.

Sample Responses

Example 1

```
{
  "brandId": "B123ABC",
  "category": [
    {
      "id": "WEB_DOMAIN",
      "displayName": "Web Domain",
      "description": "Not valid/recognised email domain",
      "fields": [
        "businessContactEmail"
      ],
      "errors": [
        {
```



```
    "code": "TFWD01",
    "message": "The submitted business contact email is not an
allowable domain."
  },
  {
    "code": "TFWD02",
    "message": "The submitted business contact email domain
ownership cannot be independently verified."
  }
]
}
]
```

Example 2

```
{
  "brandId": "B123ABC",
  "category": [
    {
      "id": "WEB_DOMAIN",
      "displayName": "Web Domain",
      "description": "Not valid/recognised email domain",
      "fields": [
        "businessContactEmail"
      ],
      "errors": [
        {
          "code": "TFWD03",
          "message": "The pin issued on the submitted business
contact email is expired without a response."
        }
      ]
    }
  ]
}
```



New Endpoints

Resend 2FA Email

POST /brand/{brandId}/2faEmail

There will be circumstances where a 2FA email needs to be sent again. This API endpoint can be invoked by the CSP to resend the 2FA email to the brand. The API request will only be accepted if all of the following conditions are met:

- Locate a past Authentication+ request with no changes to previously submitted identity fields.
- The matched Authentication+ request is still awaiting 2FA confirmation.
- The matched Authentication+ request is less than 30 days old.

On failure to meet the above conditions, TCR will respond with a Not Found error for the 2FA request.

Responses

Code	Description
204	Success
400	Request failed. Refer to the included TCR error code and message for more information. <ul style="list-style-type: none">• 501: Invalid input parameter.• 502: Brand record not found.• 565: Unable to send 2FA. Please submit brand for revet.• 590: TCR internal system error. Please contact TCR support.• 592: Operation declined. 2FA verification is already complete.
401	Unauthorized access. Check your API credentials.
429	Too Many Requests



Impacted DCA API Endpoints

Existing Endpoints

Get Brand Info by Brand ID

GET /brand/{brandId}

Public Profit entity type brands in a VERIFIED or VETTED_VERIFIED status will return several new fields in the response.

New Fields

Field name	Type	Length	Description
businessContactEmail	String	100	Brand's business contact email address. Note: Free or personal email addresses are not supported. This field will only be visible to DCAs who have signed a DPA agreement with TCR.
businessContactEmail VerifiedDate	String	N/A	An ISO 8601-formatted date and time of the successful 2FA email completion.
businessContactTitle	String	50	Job title of the brand business contact representative. Note: This field will only be visible to DCAs who have signed a DPA agreement with TCR.
businessContact FirstName	String	100	First name of the brand business contact representative. Note: This field will only be visible to DCAs who have signed a DPA agreement with TCR.
businessContact LastName	String	100	Last name of the brand business contact representative. Note: This field will only be visible to DCAs who have signed a DPA agreement with TCR.



Impacted MNO API Endpoints

Existing Endpoints

Get Brand Info by Brand ID

GET /brand/ {brandId}

Public Profit entity type brands in a VERIFIED or VETTED_VERIFIED status will return several new fields in the response.

New Fields

Field name	Type	Length	Description
businessContactEmail	String	100	Brand's business contact email address. Note: Free or personal email addresses are not supported. This field will only be visible to MNOs who have signed a DPA agreement with TCR.
businessContactEmail VerifiedDate	String	N/A	An ISO 8601-formatted date and time of the successful 2FA email completion.
businessContactTitle	String	50	Job title of the brand business contact representative. Note: This field will only be visible to MNOs who have signed a DPA agreement with TCR.
businessContact FirstName	String	100	First name of the brand business contact representative. Note: This field will only be visible to MNOs who have signed a DPA agreement with TCR.
businessContact LastName	String	100	Last name of the brand business contact representative. Note: This field will only be visible to MNOs who have signed a DPA agreement with TCR.



2FA Notification Events

The following events may occur during the course of the Authentication+ process. These events are crucial for tracking 2FA progress. TCR intends to share these events with the responsible CSP via a webhook notification.

Event Type	Event Category	Event Owner	Notes
BRAND_EMAIL_2FA_SEND	BRAND	Email service provider	This event is generated when a 2FA is sent. This does not mean the email is received by the brand.
BRAND_EMAIL_2FA_OPEN	BRAND	Email service provider	This event is generated when the brand contact opens the email. However, this event may not be produced if: <ul style="list-style-type: none">• The embedded pixel tracking code is stripped by the receiving mail server.• There is an incompatibility between the email client and the embedded pixel tracking code.
BRAND_EMAIL_2FA_CLICK	BRAND	Email service provider	This event is generated when the brand contact clicks on the Confirm button or opens the embedded link in the client-side browser.
BRAND_EMAIL_2FA_COMPLETE	BRAND	Authentication + Service	This event is generated when the brand contact completes the 2FA verification process.



BETTER MESSAGING

campaign registry

FAQ

Q. How will TCR manage email verification if a brand uses personal email addresses instead of business email addresses?

A. In the initial roll out, Authentication+ only applies to brands with a Public Profit entity type (e.g., publicly traded companies). TCR expects that all public businesses/brands will have business domain email addresses. If this is not the case, CSPs must reach out to TCR Support (support@campaignregistry.com) or submit an appeal for the identity verification request.

Q. Will TCR reject emails that start with sales@ or support@?

A. Yes. A brand's business email must be an employee's business email address and not a distribution list (for example, addresses that start with sales@ or support@).

Q. Will legacy campaigns be able to link additional numbers without going through 2FA?

A. Yes. Non-compliant legacy campaigns will be able to provision additional numbers.

Q. What will happen if a CSP resubmits an existing campaign for a Public Profit brand that is not Authentication+ verified?

A. The CSP will receive a 509 error "Brand does not qualify for submitted campaign use case." and the campaign will not qualify for new terms.

Q. When an existing brand adds a new brand business contact email, their identity status will transition to UNVERIFIED. Will number registration on the brand's existing campaigns remain functional?

A. Yes. Number registration on existing campaigns will not be impacted by the brand's transition to UNVERIFIED.

**Q. Is there a new fee associated with Authentication+?**

- A.** Eventually there will be a new fee. In the initial rollout, TCR will not be charging this fee for any brands that are Public Profit entity types. Also, TCR will refund the cost to revert existing Public Profit brands with a VERIFIED or VETTED_VERIFIED identity status that choose to go through Authentication+ verification. In later phases, as we add Authentication+ to other entity types, a new fee will be applied. The revert fee will not be applied, so it will not appear on the billing invoice.

Q. Can I whitelist the Authentication+ sender email address in my email client to make sure I receive them?

- A.** Yes. All Authentication+ 2FA emails will come from **noreply@auth.campaignregistry.com**. Please refer to your email client documentation for instructions on how to whitelist emails by sender.

Q. How can a CSP determine if a Public Profit brand has completed their 2FA verification and is Authentication+ compliant?

- A.** Authentication+ compliance is tracked by the brand attribute **businessContactEmailVerifiedDate**. If this attribute contains a date, then 2FA verification is considered complete and the brand is Authentication+ compliant. CSPs can use the **GET /brand/{brandId}** endpoint to check for this attribute for a specific brand. If a CSP wants to search all of their registered Public Profit brands and see their Authentication+ compliance, they can use the **GET /brand** endpoint.

Q. What happens if an incorrect email address is mistakenly added during brand creation? How does it get fixed?

- A.** The CSP will need to update the brand's business contact email address and resubmit the brand (via the CSP portal or CSP API).

Q. What should a CSP do if a 2FA email expires?

- A.** A 2FA email sent to a brand business contact is only valid for 7 days. After 7 days, the email link will expire and a CSP can use the CSP portal or the **POST /brand/{brandId}/2faEmail** endpoint to send another 2FA email.



BETTER MESSAGING

campaign registry

Q. What should a CSP do if a brand doesn't complete their 2FA email verification within 30 days?

- A.** If 2FA verification is not completed within 30 days of registration (for new Public Profit brands) or re-verified (for existing Public Profit brands), the CSP will need to resubmit the brand to send another 2FA email.

Q. What is the deadline to get all legacy Public Profit brands Authentication+ verified?

- A.** There is currently no deadline for getting Public Profit brands Authentication+ verified. When a deadline is established by the carriers, TCR will communicate this to customers.

Q. Will all legacy Public Profit brands change to UNVERIFIED when Authentication+ is released?

- A.** No. Legacy Public Profit brands will not automatically change to UNVERIFIED when Authentication+ is released. A brand's identity status will only change to UNVERIFIED when a brand business contact email is added. CSPs will then need to resubmit the brand and wait to get 2FA confirmation. Once confirmed, the brand will change back to VERIFIED or VETTED_VERIFIED depending on its previous identity status. Active campaigns for legacy Public Profit brands will not be affected, but to register new campaigns, the brand will need to be Authentication+ compliant. For the initial rollout, TCR will refund the cost to re-verify existing Public Profit brands with a VERIFIED or VETTED_VERIFIED identity status that choose to go through Authentication+ verification. The re-verify fee will not be applied, so it will not appear on the billing invoice.

Q. Can I customize the Authentication+ emails to match my CSP's branding?

- A.** No. Since there are possible downstream partners in the connectivity chain, it would be difficult to ensure that the correct CSP branding (from the client's point of view) is displayed in the 2FA email.

Q. What will the fee be for other brand entity types (i.e., not Public Profit) when Authentication+ becomes required in the future?

- A.** This has yet to be determined. A fee structure will be communicated to customers in a future release.

Q. When will Authentication+ verification be required for other brand entity types?

- A.** This has yet to be determined. Authentication+ verification for other brand entity types (i.e., other than Public Profit) will be communicated to customers in a future release.



BETTER MESSAGING

campaign registry

Q. What should the brand do if they do not receive the 2FA email?

- A. If the brand business contact does not receive the 2FA email, they should add the TCR email address noreply@auth.campaignregistry.com to their email system's whitelist of known addresses and request the CSP to resend the email.

Q. If a Sole Proprietor entity doesn't have a business email, how will they work with Authentication+?

- A. Currently, Authentication+ is designed specifically for Public Profit entities. When we expand to include other entity types, such as Sole Proprietors, we will implement standards that are tailored to them.

Q. Can an existing Public Profit brand make a change to their brand details without going through Authentication+ verification?

- A. No. Starting in release 5.20, existing Public Profit entities must go through Authentication+ verification if they want to add new campaigns or make any changes to their brand details.

Q. Do mock brands created in the CSP API receive 2FA emails?

- A. No. Mock brands created with the CSP API will automatically receive all events associated with successful Authentication+ 2FA verification (see the [2FA Notification Events](#) section for details), but they will not receive an actual 2FA email.

Q. Can a brand use a parent company or subsidiary company email for the business email contact?

- A. No. The business contact email address should correlate with information submitted about the Public Profit brand in order to pass verification.

Q. Will there be a refund listed on the invoice for Public Profit brands that are revetted?

- A. No. TCR will refund the cost to revet existing Public Profit brands in a VERIFIED or VETTED_VERIFIED identity status when they go through Authentication+ verification, but there will not be a specific refund listed in the invoice. The revet fee will simply not be applied.

Q. Can a Public Profit brand apply for a Standard or Enhanced vet if they are not Authentication+ compliant?

- A. No. As of December 12, 2024, Public Profit brands trying to apply for a Standard or External vet will result in an error if the brand has not passed Authentication+ verification.

**Q. How can I ensure that the Public Profit brand gets 2FA verified as quickly as possible?**

A. If there are any irregularities detected in the brand's information (or a disparity between the brand info and business contact email address), it's possible that 2FA verification will take longer to complete. This is due to manual steps that must be taken in order to verify that the brand is associated with the brand contact email address. To expedite 2FA verification, CSPs should ensure that:

- The brand's EIN belongs to and is associated with the legal entity that's submitted.
- The official domain of the legal entity matches the domain of the business contact email address.
- The brand's website domain has been submitted as part of the brand information and matches the official domain of the legal entity.
- The stock symbol in the brand information is correct.
- The stock exchange in the brand information is correct.

Q. What should I do if the brand's business contact receives an error message when they click the link/button in the 2FA email?

A. If the brand contact gets the message "Link has expired:"

- If the Authentication+ 2FA request is less than 30 days old:
 - Resend the 2FA email via the CSP portal or CSP API. 2FA email links expire 7 days after they have been sent. They can be resent within 30 days of the original 2FA request.
- If the Authentication+ 2FA request is more than 30 days old:
 - Resubmit the brand. This will restart the Authentication+ process and a new 2FA email will be sent.

If the brand contact gets the message "Brand contact email verification could not be completed," try the following:

- Click on the link again. The first attempt may not register properly.
- Copy and paste the link URL into an incognito browser and try again.
- Ask the brand's IT/InfoSec team to whitelist the <https://verify.campaignregistry.com/> domain and try again. Some internal IT systems block unknown URLs to help prevent information breaches.
- If the previous suggestions don't work, try resubmitting the brand or contacting TCR Support (support@campaignregistry.com).

If you encounter any other issues, try resubmitting the brand or contacting TCR Support (support@campaignregistry.com).