PLAID

Plaid Identity Verification + Monitor

Recommendations and helpful tips for building your KYC and AML solution

This guide outlines best practices and suggestions for building a user friendly identity verification solution which allows good users to seamlessly onboard onto your platform while keeping bad actors out. We've broken this down into key considerations as you work to configure your dashboard, integrate with our solution, understand pass/fail logic, and leverage the resulting data.

Please note:
The suggestions in this guide are not legal or compliance advice. Please consult with your legal or compliance team regarding your legal obligations and AML compliance program.

Table of contents

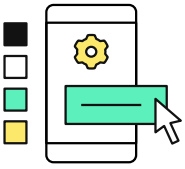
Introduction

There are multiple verification aspects of the IDV and Monitor solutions which allow you to verify your users in accordance with your compliance needs. The main pieces of the solution to understand before you dig into the below guide are:

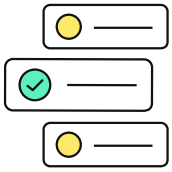
- **Lightning check:** This is part of our IDV solution. A user inputs their PII via our Link module and we verify that data against regulated databases. You can also send us some or all of the PII via API which we'll explain in this guide.
- **Document verification:** This is the second part of our IDV solution. A user interacts with our Plaid Link module to upload a document. We then verify the validity of the document and that their information matches the inputted PII (Name + DOB). We require the user to take a photo and upload the document in real time to minimize fraud from uploads from repositories of fake documents.
- **Selfie check:** This is the last part of our IDV solution where a user takes a short video which confirms liveness and is verified against their document image.
- **AML screening:** This is part of our Monitor solution which allows you to screen a given user's name against a variety of watchlists to confirm that you can do business with this user.

Configure your dashboard

The Identity Verification and Monitor dashboard is your one-stop-shop for building your KYC solution. The dashboard is designed to allow you to easily customize and adjust your identity verification solution. A few of the key things you're able to do on the dashboard include:



Customize the end user experience



Configure your verification rules and AML settings

Review completed verifications and screening hits

Below, we'll walk you through what to be aware of when configuring your Identity Verification templates and Monitor programs.

Identity Verification templates

The IDV templates allow you to configure the end-user verification experience while also inputting your compliance rules to determine how a user is able to pass KYC.

CONFIGURE YOUR FIRST TEMPLATE

1 Create a new template

- On the Identity Verification section of the dashboard click on “New Template”.

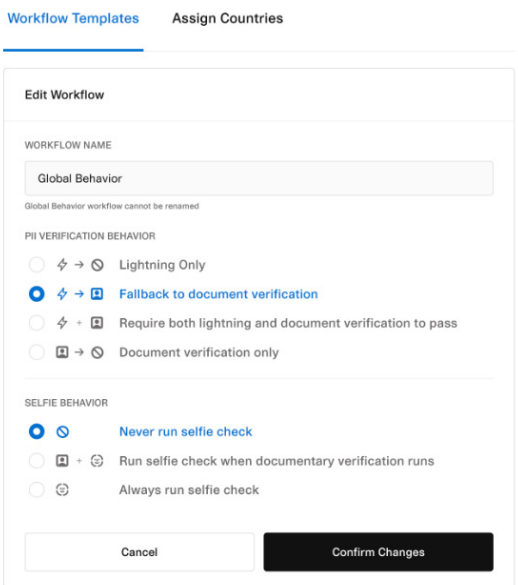
2 Fill out the basics

- Name your template! Also make sure to select your industry and populate your privacy policy link.
- Enable the Auto-fill feature, if desired. You can read more about this in the ‘Additional Identity Verification considerations’ below.
- If you’re also leveraging AML screening, check the box and determine what program you want to use to screen your users.
- Use SMS verification to seamlessly confirm your end users’ phone numbers at no additional cost.

3 Customize the design

- Input your primary color and logo to make the experience feel familiar to the user.

4 Set the end user workflow



This is where you determine what verification methods end users will experience. The options available to you are:

Leveraging multiple templates
If you require different workflows or risk rules for different user types within the same country, you should create multiple templates. For example, you could have one template specifically for high risk users where you require document verification and selfie, and another for lower risk users with just a lightning check.

- **Lightning Only:** Only perform a PII verification on the user to determine whether they pass or fail KYC.
- **Fallback to document verification:** Perform a PII verification on the user, if it fails (based on your rulesets), then we will ask the user to upload a document. This can then be used as another piece of data to verify the user.
- **Require both lightning and document verification to pass:** We will always perform both a PII verification and document verification on the user.
- **Document verification only:** We will not perform a PII verification but will require them to upload a document. However, we still require the user's PII to compare it to the document. More data on this can be found in the additional considerations section below.
- **Selfie behavior:** Here you can choose whether you want us to do a liveness analysis on the user whenever they upload a document, always, or never.

You can configure different workflows which can be assigned to different countries in the Assign Countries tab. This is also where you can determine which documents you want to accept for each country and where you can decide whether to verify full 9 of SSN, last 4 of SSN, or skip SSN verification entirely.

5 Build your identity rulesets

- Work with your compliance team to set up the definition of a successful verification. We will check the identity rules for each user that verifies their identity to determine if a user passes or fails.
- This ruleset builder leverages boolean logic to allow you to have multiple rules if you have multiple ways to satisfy your requirements. We will check each requirement on your first rule and if all of those are met, then the KYC check will be successful. If not, we will progress to your second rule.

6 Set your risk thresholds

- We will calculate risk levels for each user based on multiple factors which we will explain in the Additional Identity Verification considerations below.
- We recommend starting with a Medium risk level and adjusting over time.
- **Note:** When testing in sandbox, it is common to trigger the Identity Verification Network and Device risk due to repeated testing from the same network or device. To bypass this, you can set your Network and Device Risk thresholds to High in your sandbox template. Make sure to edit this when you create your production template, though!

7 Integrate your template for end users

- You're ready for users to use your template! We'll walk through how to launch this template as part of your application in the second section of this guide.

Support for ITIN and ATIN

We support verifying a user's ITIN or ATIN identification number in place of their SSN. The user can simply enter this as their SSN in the IDV modal. If you're sending us this data on the backend, you can set id_number.type = us_ssn or us_ssn_last_4, respectively, and we'll automatically handle the ITIN or ATIN.

ADDITIONAL IDENTITY VERIFICATION CONSIDERATIONS

Auto-fill functionality

Autofill expedites the verification experience by populating additional identity information that's associated with a user's phone number and date of birth. After entering phone number and date of birth in an IDV session with SMS verification enabled, you now have the option to let Plaid autofill additional identity information like full name, address, and SSN. We will allow the user to confirm their autofilled information is accurate before submitting. Additionally, if autofill fails for any reason, the user is seamlessly transitioned to the classic IDV flow. Please note that you must enable SMS verification to leverage autofill.

Document only workflow

If you're looking to just verify documents for your users and leverage the document-only flow, you should note that we still require the PII for the user. This is because we cross-reference the document data with the PII information to verify a user with this method. Therefore, we'll ask the end user for their PII unless you pre-pass that data to us. You can see more information on that by checking out the Hybrid link flow integration method below.

Selfie behavior

The selfie feature allows you to confirm that the end user is a real person and matches the document they uploaded. You can configure in your workflow whether you want to never ask for selfie, always ask for it, or only ask for it when the user uploads a document.

Risk categories

We calculate five different risk categories to support your fraud prevention efforts. We look at many factors to determine a risk level, some of the key things we look at are:

- Phone Risk: External account connection, etc.
- Email Risk: Email deliverability, disposable emails, data breach checks, etc.
- Network Risk: Fingerprint session and analyze risk based on previously seen traffic.
- Device Risk: Proxy, VPN, Tor browser, abuse lists, etc.
- Behavior Risk: Analyzes user behavioral attributes during sign up process.

Language support

Plaid's Identity Verification modal will automatically detect a user's browser language and adapt the experience to the correct language. As of Q1 2023, we currently support English, French, Spanish, Portugese, and Japanese, with more languages on the horizon. We also offer a language select dropdown on the IDV modal in the case where a user may want to switch to a different language. Please note, passing a language via link/token/create call will not alter the above experience.

Should I use ongoing monitoring?
Ongoing monitoring is highly recommended when you have an ongoing relationship with your users. One way to configure this would be to set up two programs - one with ongoing monitoring enabled and one without. As users onboard to your platform screen them in the program without ongoing monitoring, and move them to the other program once you know you will have an ongoing relationship with them.

Monitor programs

The Monitor product allows you to easily create an AML screening program for your users that minimizes false positives and handles case management when you get hits. We provide screening both for individuals and for entities - we've separated these on purpose to ensure the hits you get are high quality.

CONFIGURE YOUR FIRST PROGRAM

1 Create a new program

- On the Monitor section of the dashboard click on "New Program" to screen individuals or "New Entity Program" to screen against entities.

2 Set up ongoing monitoring

- Having ongoing monitoring turned on will screen all your users against your enabled watchlists on a daily basis, and will automatically account for any changes to those watchlists.

3 Configure your name sensitivity

- Set the level of name sensitivity you'd like for your screening matches. The more exact (to the right) you go, the less false positives you'll get but will also increase your risk of missing a hit. For detailed information on how this works, take a look below at the Additional Monitor Considerations section.
- Plaid Monitor is built to make it difficult to overconstrain a search and therefore have false negatives. That being said, if your data inputs are not quality controlled to at least a basic extent prior to sending them to us, this can result in false negatives or false positives (for example, broad searches based on incomplete names).

4 Adjust date of birth filtering

- Date of birth filtering provides an additional data point to reduce noise in your screening program. We recommend you filter by date of birth to limit false positives of your program.

5 Define case review behavior

- The dashboard has built-in case management to help you handle all hits you receive. You can add all users you want to be part of the review team in the user program access section.
- Determine how you want to allocate new hits to your team - you can either assign them to an analyst at random or leave them unassigned in a queue for people to pick up as they can.
- You can also configure secondary reviews in the case of a hit under certain conditions set by you. You can also set case management such that the secondary review must be done by a manager by enabling "prefer escalation".

6 Set your watchlists

- Enable the watchlists you want to screen your entities or individuals against for this program. There is no incremental cost based on the watchlists you enable - they are all included!

7 Configure PEP screening

- For individual-based programs, we allow you to screen your users against Politically Exposed Persons lists.
- As you increase in level, your likelihood of false positives significantly increases.

ADDITIONAL MONITOR CONSIDERATIONS

Name sensitivity calculations

The name sensitivity you set has a direct impact on the type of hits you get. The different levels do not turn on or off any of our fuzzy matching features, but they limit results based on a score we compute internally. We have tuned the sensitivity levels and strongly recommend you try Balanced and adjust from there.

We have many algorithms that take into account things like: normalization (lower case vs. upper case, stop words like Mr., Dr., etc), phonetic similarity, complete mismatches on parts of the name, reversed orders, initialisms, gender adjustments, and many more. Each type of matching phenomenon will have a different impact on the overall score, based on the importance of the discrepancy, the length and composition of the name being verified, and other variables like language. For example, “Mr. John Doe” vs. “John Doe” will receive a negligible penalty, whereas “John Paul Doe” vs “John Doe” will receive a more significant penalty. This means there isn’t a hard differentiation between the different levels, they just set different thresholds based on the scores that get computed internally.

The ranges are currently [0.7, 0.8) for Coarse, [0.8, 0.9) for Balanced, [0.9, 1.0) for Strict, exactly 1.0 for Exact. These scores can be equated to scores similar to what you may have used with other solutions:

- **Coarse:** Minimum score of 70
- **Balanced:** Minimum score of 80
- **Strict:** Minimum score of 90
- **Exact:** Exact score of 100

That said, setting the scores at the same level between different solutions will not necessarily yield the same results, as the underlying fuzzy matching algorithms would need to be the same across the board. We believe our algorithms are much more sophisticated than many competing solutions which results in fewer false positives, while ensuring that no relevant hits are missed. Thus the numbers above can be used as a reference point, but we strongly suggest starting at a Balanced sensitivity level, and adjusting up or down from there.

PEP risk levels

When setting your desired PEP risk level to screen individuals against, the higher the selected risk level, the higher the number of positions that will be considered (and in turn the higher the number of potential hits that will be returned). Each time you go up in risk level, all of the positions/titles from previous levels will still be included, in addition to the ones specific to the level selected. Below, you can find the type of positions included in each level:

Level 1: Judge, Politician, Military Official, Central Bank Executive

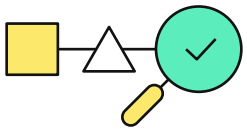
Level 2: Level 1 *plus* Executive Auditor, Administrative Office Executive, Relative/Close Associate, State Owned Enterprise Executive

Level 3: Level 2 *plus* State Owned Enterprise Executive

Level 4: Level 3 *plus* International Organization Official

Adjusting a live program

Once a program is live, any changes to that program have the potential to cause a new influx of hits, especially if you leverage ongoing monitoring. For example, if you decide to make your name sensitivity less sensitive or increase a level of PEP screening, this could cause many new hits to be picked up the next time we run that ongoing screen. Please be aware of this when modifying a program.



Hybrid Link flow with conditional Link

Note: If you are leveraging Hybrid flow with the workflow setting 'Fallback to document verification' and you are pre-passing us all PII fields, then you will only need to launch Link to the user if they fail the KYC check. Therefore, you'll want to listen to check the outcome of the KYC step and use that as a trigger for further end-user interaction.

Integrate the solution

Core integration types

Our goal is to have this solution be adaptable to your use case and desired user experience. As such, there are a few different ways you can integrate the IDV solution into your product:

1. Full Link flow (no pre-passed PII): In this style, the end user interacts with the Plaid Link module to input their PII data as well as upload a document and take a selfie, if needed. In this flow, we ask the user to enter all of the PII data we need for verification: name, address, phone number, DOB, and SSN (based on your settings).
2. Hybrid Link flow (partial pre-passed PII): In this flow, you pre-pass us any existing PII you have on the user before they go through the Plaid Link module. We will dynamically adapt their Link experience to only ask for the fields of PII you do not already have. The user can also upload a document or run selfie verification in Link based on your workflow.
3. Hosted Link flow (shareable url): In this method, we will host the Link experience for you to verify your users - you do not have to worry about launching Link via your own front-end. We will generate a shareable url that you can then send to your users as you'd like.
4. Back-end flow: In this flow, you send us all the key PII fields via API and we return the status of the verification to you without the user needing to interact with Plaid Link. This method is available if you are running only a lightning (PII) verification, do not need SMS verification, and have already obtained consent from your users.

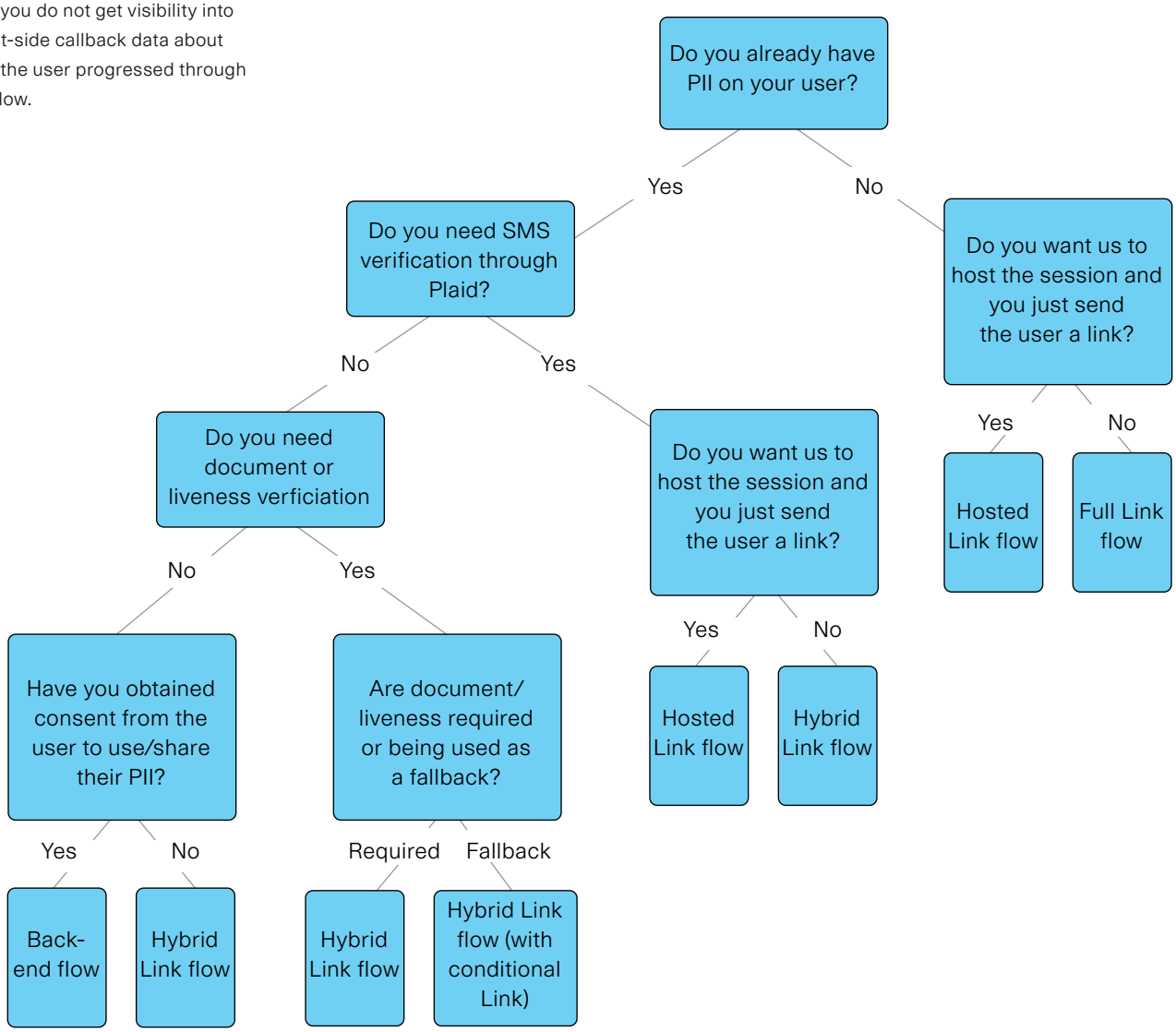
For our Monitor solution there are two main methods to integrate:

1. Alongside IDV: If you are leveraging our IDV solution, you can have all your users automatically screened through a desired AML program without needing to make any additional API calls. You can configure this in the dashboard when you set up your IDV Template.
2. Standalone screening: If you are not leveraging IDV, you can use our API to run your users through a configured AML program.

Note: Hosted link is best used when you need to send your user a link to complete verification. If you want IDV as part of your core application flow, you should likely host Link yourself. Also, with the Hosted Link flow you do not get visibility into client-side callback data about how the user progressed through the flow.

How to pick your integration type

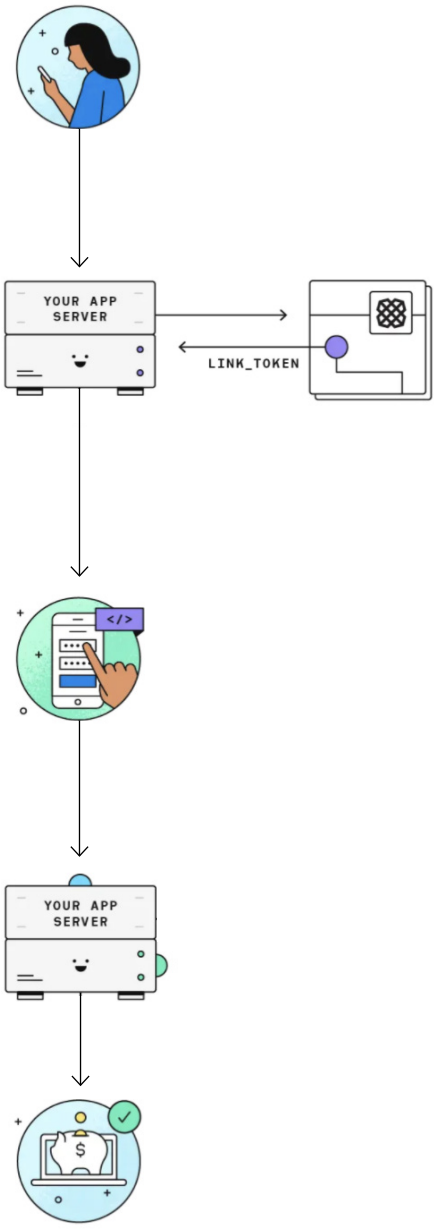
Your integration type is based in part on your desired user experience but also on the features you want available. Take a look at the decision tree below to give you an idea of some of the key considerations when determining your integration type.



Integration schemas

The API calls you make vary slightly depending on your integration type. Please find below integration sequences for each type of IDV Integration.

Full Link flow



1 Make a request to create a **link_token** via the /link/token/create endpoint. Set products = identity_verification, supply the template_id and client_user_id, and optionally an email to allow us to run additional risk checks.

2 Use the link_token to open Link for your user. Listen for the onSuccess callback which will let you know that your user has successfully completed the session. Make note of the link_session_id (which is also the identity_verification_id).

3 We will also inform you of the status of the verification via identity_verification webhooks. You should listen to these as well.

4 Call the /identity_verification/get endpoint to view the outcome of the verification and granular insights into each step.

Hybrid Link flow

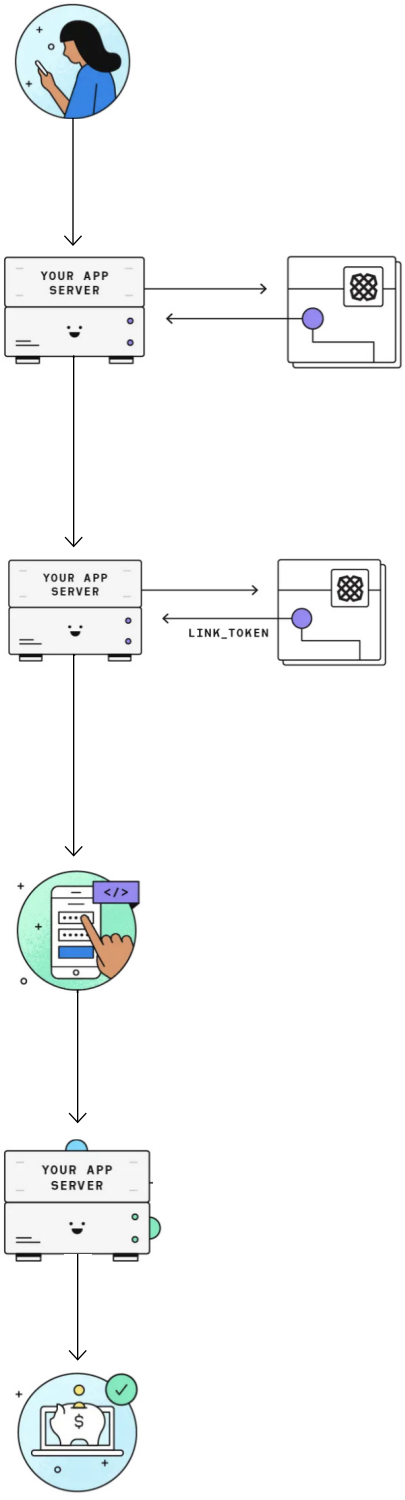
1 Call identity_verification/create with a given template_id and client_user_id. Provide any data you have for your user and we will adjust our UX based on what you send us to create a seamless flow.

2 Make a request to create a link_token via the /link/token/create endpoint. Set products = identity_verification, supply the template_id and client_user_id you passed in the create call in step 1.

3 Use the link_token to open Link for your user. Listen for the onSuccess callback which will let you know that your user has successfully completed the session. Make note of the link_session_id (which is also the identity_verification_id).

4 We will also inform you of the status of the verification via identity_verification webhooks. You should listen to these as well.

5 Call the /identity_verification/get endpoint to view the outcome of the verification and granular insights into each step.



Shareable Link flow

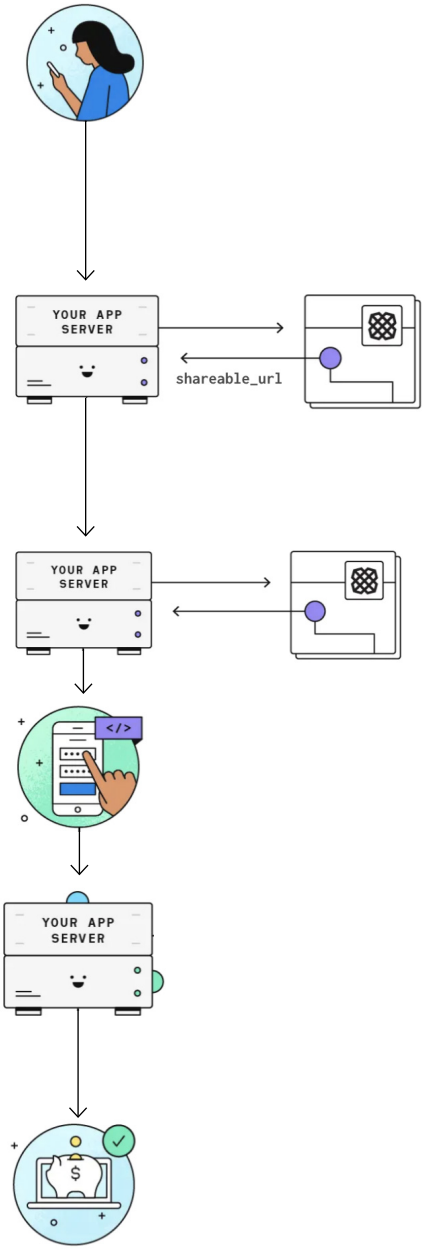
1 Call identity_verification/create with a given template_id and client_user_id. Provide any data you have for your user and we will adjust our UX based on what you send us to create a seamless flow. Set is_sharable = true.

2 Receive the shareable link and pass it to the user as you see fit. This could be done via text or email for example.

3 User will interact with our Plaid-hosted Identity Verification link experience.

4 We will inform you of the status of the verification via identity_verification webhooks. You should listen to these.

5 Call the /identity_verification/get endpoint to view the outcome of the verification and granular insights into each step.



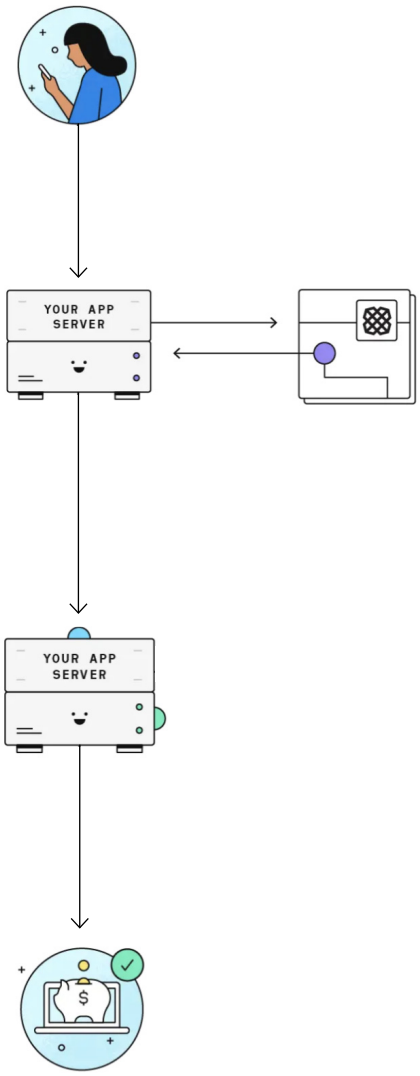
Note: To successfully complete a back-end flow you must send us all data on your user. This includes: full name, date of birth, phone number, address, and national identifier (ie. SSN) if required in your dashboard settings.

Back-end flow

1 Call identity_verification/create with a given template_id and client_user_id. Provide all the data you have for your user. Indicate whether you've obtained consent and make sure sms verification is turned off on your dashboard template.

2 Wait a few seconds for the verification to complete. We will also inform you of the status of the verification via identity_verification webhooks. You can consider strategic polling if you don't receive the data right away but we strongly recommend listening for webhooks.

3 Call the /identity_verification/get endpoint to view the outcome of the verification and granular insights into each step.



Meanwhile for the Monitor flow, there are two main integration flows based on whether you leverage our IDV product or not.

If you leverage IDV:

1. Set up your program as highlighted in the Configure your dashboard section. Then, when you set up your IDV Template, be sure to select the AML Screening, 'screen customers' checkbox to automatically screen all users that go through IDV through your program.
2. Call the identity_verification/get endpoint. You will be able to see the status of the screening. If the user has a hit, they will be put into a pending_review status.
3. If you have ongoing monitoring configured, we will inform you of any future hits via a SCREENING (or ENTITY_SCREENING) webhook. You can view hits in the dashboard by checking the Pending Review queue. We also recommend configuring an alert for reviewers based on this webhook.

If you do not leverage IDV:

1. Set up your program as highlighted in the Configure your dashboard section.
2. Call the watchlist_screening/individual/create (or */entity/create) to screen a user/entity. More details on this endpoint can be found here.
3. You will see the status of the screening in the response from the endpoint. If the user has a hit, they will be put into a pending_review status.
4. If you have ongoing monitoring configured, we will inform you of any future hits via a SCREENING (or ENTITY_SCREENING) webhook. You can view hits in the dashboard by checking the Pending Review queue. We also recommend configuring an alert for reviewers based on this webhook.

Testing

There are two environments you can test IDV + Monitor in: sandbox and production. Note that we do not support the development environment for these products. In sandbox, you can leverage dummy data to test your IDV workflows while in production you can test with real data. In the sandbox, we've configured a sample test user that will allow you to pass verification checks. Here are a few things to keep in mind as you test the product:

Lightning verification: The matching logic is fully functional even in test mode. Since the same identity record is always used when in test mode, you can adjust your search input to simulate different outcomes at the attribute level, and then set up different match rules to simulate different outcomes at the overall lightning level based on individual attribute match statuses. Example: If you search by the exact same name as the one contained in the test record, you will get a match on name. Include a typo in the name input, and you will get a partial match. Use a completely different name, and you will get no match. The same logic can be applied to any of the attributes. By modifying the sample record to use a search input, you should be able to simulate any outcome you'd like to test for. Additionally, autofill behaves the same in sandbox as in production, albeit with the test record of Leslie Knope.

Need a user to try again?
If a user failed their verification and you'd like them to try again, you can use our retry functionality! To do this, call the /identity_verification/retry endpoint with their client_user_id and template_id. You can modify the strategy and steps fields to determine what parts of the verification you want the user to retry. Then, launch Link as you normally would! You can also do this from a user's record directly in the dashboard by clicking on 'Request Retry'.

Document verification: In sandbox, what determines whether the document step passes or fails is the name and date of birth comparison check only. The sandbox environment acts as if the information extracted from the document is Leslie Knope, with a DOB of January 18th 1975, and it expects the user-provided input to be the same. If that is the PII provided, the comparisons will succeed. If not, they will fail.

Liveness: Liveness is not currently part of the sandbox environment, so there is no testing option. The template editor will let you configure your workflow to require selfie verification, but the session itself will never prompt you for it, nor will the verification report include that step.

Watchlist screening: If the name entered in the original data collection phase is a name that is listed on any of the watchlists we support and you are screening against, you will be able to simulate a case of a watchlist hit being surfaced, and the user being thrown into pending review. From there you will be able to navigate to the associated screening which is located in the Monitor tab of the dashboard, and resolve that screening, which will in turn resolve the identity verification session. Please note that entering a name that would trigger a watchlist hit means you are not entering "Leslie Knope", which means you would fail the document verification step (because of the name comparison check).

Risk check: An easy way to trigger a failure on the risk step is to leverage the Identity Verification Network risk check. This check looks at the user's device fingerprint and checks whether that device has been seen before on our network verifying an identity (any identity). If you create multiple test sessions from your same device, the risk level for that section will go up. If you set the acceptable risk level for it to "Low", that will result in you failing the risk step as a whole. Please note that when testing in sandbox, it is common to trigger the Identity Verification Network and Device risk due to repeated testing from the same network or device. To bypass this, you can set your Network and Device Risk thresholds to High in your sandbox template. Make sure to edit this when you create your production template, though!

Leverage callback data

When you use our Plaid Link module, we'll fire client-side callbacks to inform you of how your users are progressing through the flow. Please note that you will not be able to access these if you use the hosted experience with shareable links. That said, there are a few types of events to listen for:

1. **onSuccess:** This will let you know when your user has successfully completed the IDV flow. Make note of the link_session_id as this is equal to the identity_verification_id. You'll need this identifier to call the /identity_verification/get endpoint.
2. **onExit:** This will let you know that a user exited the session without finishing all required steps. You may want to listen for this and prompt the user to finish the KYC process.
3. **onEvent:** These callbacks will let you know the progress the user is making through the flow and can be fed into data and analytics tools. For each step, we will send an IDENTITY_VERIFICATION_START_STEP event as well as a IDENTITY_VERIFICATION_PASS_STEP or IDENTITY_VERIFICATION_FAIL_STEP event based on the outcome of the step. The possible types of steps are:

- ACCEPT_TOS - Accept terms of service
- VERIFY_SMS - Verify phone number
- KYC_CHECK - Enter PII for the lightning verification
- DOCUMENTARY_VERIFICATION - Upload document
- RISK_CHECK - Run the risk checks based on the user
- SELFIE_CHECK - Take a selfie video for liveness check

For each session, we will also inform you of the outcome of the session by sending an IDENTITY_VERIFICATION_PASS_SESSION or IDENTITY_VERIFICATION_FAIL_SESSION based on the outcome of the session.

Webhooks

As a key part of your integration, you need to add a webhook receiver endpoint to your application. First, visit the dashboard webhook configuration page and click New Webhook.

You can select which events you want to subscribe to. For Identity Verification, there are three events:

- STEP_UPDATED
- STATUS_UPDATED
- RETRIED

Enter your webhook receiver endpoint for the webhook you wish to subscribe to and click Save. Plaid will now send an HTTP POST request to the webhook receiver endpoint every time the event occurs.

Additionally, it is important to note that Identity Verification does not guarantee that webhooks will be delivered in any particular order. For example, while the logical ordering of webhooks for a Identity Verification session might look like this:

1. STEP_UPDATED - The user has started the Identity Verification session and is on the first step
2. STEP_UPDATED
3. STATUS_UPDATED - The user has reached a terminal state for their session
4. RETRIED - A retry has been requested for this user, either via the dashboard or via API
5. STEP_UPDATED
6. STEP_UPDATED
7. STATUS_UPDATED - The retry has been completed

You should be prepared to handle these events in any delivery order.
For example, consider whether your application will properly handle:

- A STEP_UPDATED event being delivered after a STATUS_UPDATED event.
- A STEP_UPDATED event being delivered before an associated RETRIED.

Best practices

Make use of client_user_id

At the center of Plaid IDV and Monitor is the mandatory “client_user_id” field, which we expect will be a unique and persistent identifier for your customer, ideally something like the id field on your users table. Plaid IDV intelligently handles sessions being started with the same client_user_id multiple times. If your customer starts a session, closes the page, reopens it, and reopens your IDV integration, their session will resume from where they left off. Likewise, if your customer has completed their session in the past (by either failing verification or passing), we will not serve them another session unless you’ve manually authorized another attempt from our dashboard. Further, we index the client_user_ids you send us, so that you can search on the dashboard using your internal id.

Provide email

While the field is optional, we highly recommend providing it. Plaid IDV will include the user’s email in the IDV session and perform a number of anti-fraud related checks, including:

- Checking if the email is registered with 20 different popular social networks.
- Inferring how long the email has been in use, by checking for its presence in past data breaches.
- Checking for signs of fraud and abuse, like whether the email is disposable, recently registered, or not configured to accept email.

Leverage multiple programs

The number of programs you wish to maintain will vary based on the complexity of your organization. Some common ways of splitting up programs are by product vertical (“Cardholders”, “Personal Loans”, “FDIC Accounts”, etc), geography (“US Cardholders”, “European Cardholders”, etc), risk level (“High Risk Individuals”, “Medium Risk Individuals”), or a combination of the above. For ideas about how to split customers up by risk, OFAC has prepared a helpful risk matrix that can provide a baseline for setting initial risk level and then modifying the risk level based on ongoing user behavior.

Common pitfalls

Equating no data with no match

Not all entries provided by various governments and list issuers have the same level of data richness. Some will have names, dates of birth, passports, and addresses associated with them, and others will only have names. When you are building your matching logic, make sure to take into account that no_data is different from no_match. no_data means that the list issuer didn't supply data against which to match. no_match means that data was provided by the list issuer and it did not match the information provided by your customer.

Saving a template and not publishing it

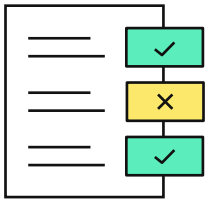
You'll notice that while editing a template there is both a 'Save Draft' button and a 'Publish Changes' button. Your template and any changes you make to it will only go into effect once you click on 'Publish Changes'.

Using the wrong template_id

The template_ids are different between sandbox and production. Make sure you are using the correct one based on the environment you're testing in.

Not asking for correct Liveness Permissions

When you use our liveness solution, you need to make sure you are asking for the correct permissions to allow your users to take a video. If you are integrating through a webview, make sure to handle mobile permissions. Also, you'll want to make sure to set allowsInlineMediaPlayback to true.



Understand pass/fail logic

It is important to understand how we determine someone has passed each of the various verification steps before you leverage the data. We've broken down how we do this for each step below.

SMS verification

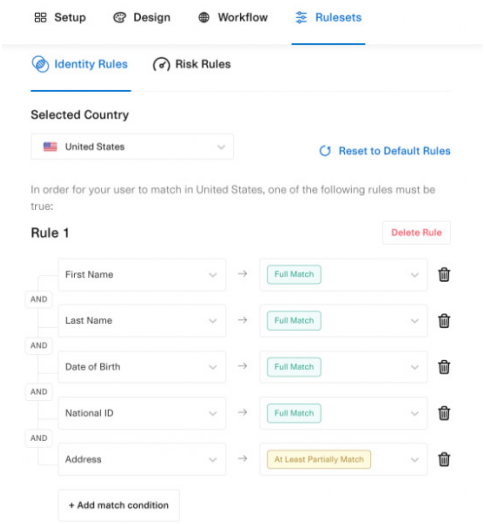
Verify customers' phone numbers by sending them an SMS code before collecting more data. Highly recommended if you do not do SMS verification somewhere else in your verification process. Required if PII auto-fill is enabled.

Verify phone number with SMS

There are two ways the SMS verification step could be failed:

1. An invalid phone number was entered twice. There are field validation checks in place to prevent the user from submitting obviously invalid phone numbers in the first place (invalid area code, invalid length, etc), but it is possible that a phone number passing our validation checks is entered, yet it is not possible to deliver to it.
2. A valid phone number was entered, and the one time passcode (OTP) was delivered successfully, but the user entered the wrong OTP into IDV UX three times in a row.

Lightning (PII) check



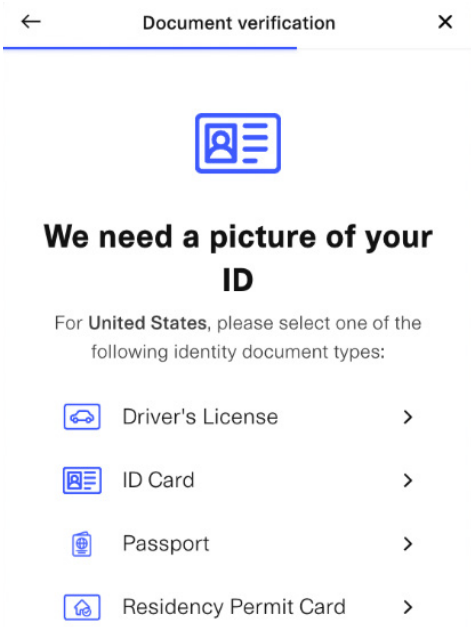
The user-submitted PII will be compared against authoritative data sources to determine whether a matching identity record is found, and if so, whether the input matches the information found in that identity record. Each attribute will be scored by our matching algorithms, and will receive one of the following flags: match, no match, partial match, not found. Whether the overall lightning step passes or fails will be determined by the identity rule(s) you set in the template editor.

Document verification check

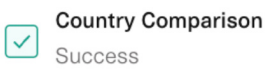
There are several requirements that need to be met in order for the document verification step to pass:

1 As part of the analysis we run on the user-submitted document, we extract information off of it and return it to you. This includes full name and date of birth, which we compare against the name and date of birth provided by the user during the initial PII collection step (or the user data passed by our client via API if that applies). **The name and date of birth comparisons must both match.**

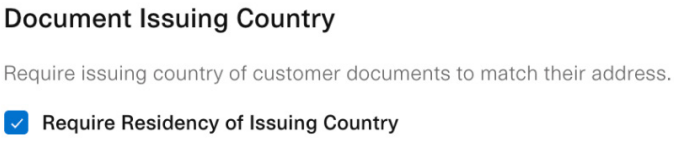
2 The ID type that is recognized by our system must match the ID type selected by the user when going through the verification UX.



3 The issuing country that is recognized by our system must match the country selected by the user from the country dropdown at the beginning of the flow.

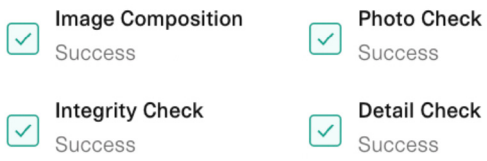


Note: This criterion only applies if the associated setting is selected in the template editor (In the Workflow tab).

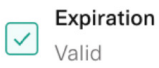


4 The various anti-fraud checks we run must all pass. Those include (subject to change):

- **Image composition:** Detects whether a submitted photo contains a physical identity document, as opposed to a scanned document or a picture of a document displayed on a screen.
- **Photo check:** We check each document to ensure the user's photo is in compliance with the requirements for the given document. For example, many identity documents require a specific contrast to highlight skin tone, removal of glasses, and a specific pose. Failing this check can mean the document is forged or otherwise tampered with.
- **Integrity check:** We check that the document is not damaged or tampered with.
- **Details check:** We check each document's details to ensure they match the jurisdiction's template. For example, field alignment, coloration, and identifying symbols.



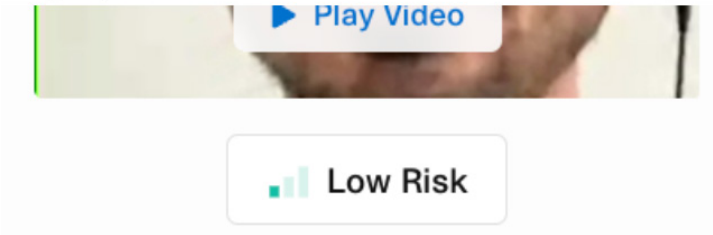
5 The document must still be valid, i.e. not expired.



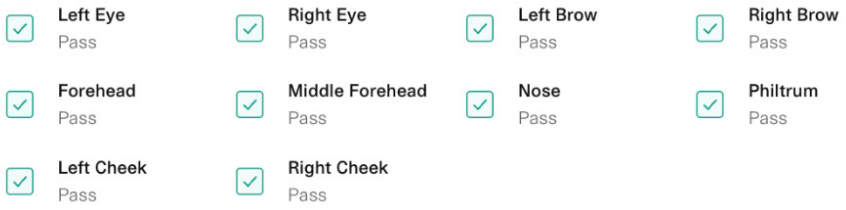
Liveness check

There are two requirements that need to be met in order for the liveness step to pass:

1 **The risk level must be low.** This risk flag is what will be triggered if the AI engine detects anything abnormal suggesting that the user may be wearing a mask, or presenting a picture of someone else to the camera, etc.



2 If an ID document was provided, a comparison is run between the picture extracted from the document, and the face captured during the liveness step. The overall comparison must be a match. 12 facial attributes are considered, and the status on each comparison is shown in the dashboard.



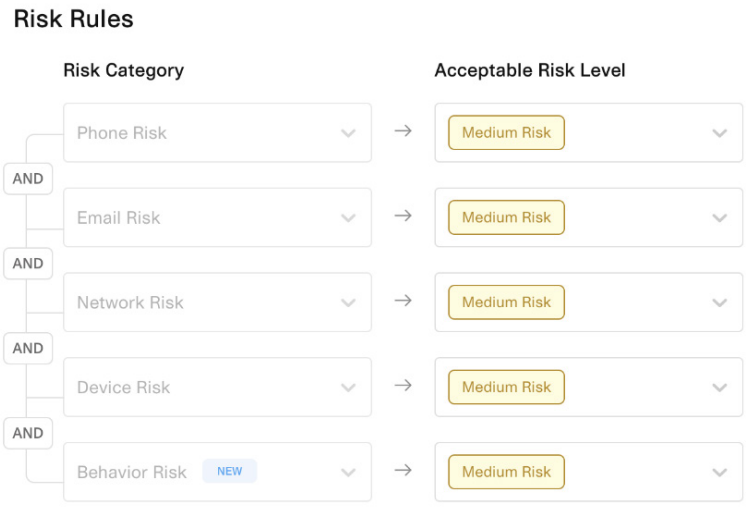
This step can also be failed due to the user not following the instructions (presenting their head in the right place, smiling when prompted).

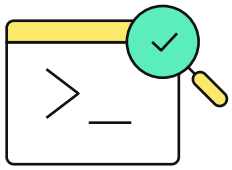
Watchlist screening

This step will never automatically fail, but it is also the only step that can end up in a pending_review state, and in turn can cause the session as a whole to be in a pending_review state. In most cases, the screening will not surface any hits, but in the event that it does, the session will be put in pending_review. You can then resolve the screening in the Monitor dashboard (there is a direct link to the associated screening in the IDV report), which will in turn resolve that step in the IDV session. If the hit(s) is confirmed and the user is rejected, the watchlist screening step will fail. If the hit(s) is dismissed (i.e. it was determined to be a false positive) and the user is cleared, the watchlist screening step will pass.

Risk check

There are a vast number of ways this step could be failed since we run a host of anti-fraud checks on the backend, but at a high level: there are five risk categories, and we assign a risk level to each of those categories (low, medium, or high risk). You set your acceptable risk level in the template editor, under the Rulesets section. If any of the risk categories get assigned a level of risk that surpasses the acceptable risk level set by you, the risk step will fail.





The power of status
The status field from the API response should be used to make a decision on what happens to the user next. The proposed logic based on status may look like:

success:
The user successfully passed KYC and can proceed in your application.

failed:
The user failed your KYC process. You can look at the steps status to understand why. The solution was designed to automatically handle most users based on the rules you've set, removing the need for manual review in most cases. However, you may consider stepping them up into a secondary KYC process or allowing them to retry if you wish.

pending_review:
The user has a potential watchlist hit. Have someone log into the dashboard to review the hit. You can also leverage our monitor endpoints if you want to see the hit information via API.

Leverage the data

Now that a user has gone through your KYC process using Plaid, you have access to key pieces of data regarding their identity that you can leverage to determine what the user should do next in the flow. There are numerous ways you can access and act upon this data shown below.

Call our APIs

Once a user has gone through your KYC flow, the outcome of their session will likely impact their next interaction with your product. There are a few ways you should consider leveraging our APIs for your key decision points:

1. Understand the session outcome: Call the /identity_verification/get endpoint to view the key data on the KYC session. Here you can find the overall status of the session, the status of each step of the verification, the data the user entered, which pieces of data were able to be verified, and the source document photos, among other things. The status field will likely impact what the user sees next.
2. Pull data into your systems: You can use the API endpoints to download key pieces of verified data you'd like to store in your systems. For example, if you want to surface the KYC status in your other systems you can do so. Also, you can use our response to view the document images the user took if you want to download those.
3. Determine which sessions to look at in dashboard: You can choose which sessions you may want to dig into in the dashboard based on certain fields we return in the api response. For example, if you see the risk_check step failed you may want to look into the dashboard to understand why or if the status is pending_review you will want someone to further investigate the session in the dashboard.

Use the dashboard for data review

The dashboard is intended to be your homebase for your Plaid KYC and AML solution. As such, you can see all data on the user directly in the dashboard. While our API response is robust and you'll likely want to automate your decisioning using our API, there are a few things that can only be seen on the dashboard. Some of the key items are:

- Liveness video check and comparison on the user if you leverage our Selfie Check.
- Granular details about risk analysis for each category.
- Social media related accounts.
- Related sessions by device id and ip address.
- Full analysis on document.
- The ability to override a failure into a success.

Configure AML review alerting

Plaid Monitor supports ongoing daily rescans of your entire customer base to alert you when new hits are discovered. This system is designed around the concept of a living pending_review queue that is updated whenever new hits are found. We will inform you via webhook when you receive a new hit, and this can be used to configure an alert for someone that they should check the pending_review queue. You could also set up a daily job to check this endpoint once a day to poll any of the screenings that end up in this queue and use the associated client_user_id to tie it back to your internal database to determine if action is required.

Please note that adding Plaid Monitor is not the only part of a successful Anti-Money Laundering program. We highly recommend that you consult with an AML professional to help you build all of the policies and procedures required. AML regulations vary widely for different jurisdictions and industries.