Identity Verification and Assurance Strategies Playbook

Requirements and Specifications for Affirm Deployment

Introduction

HYPR Affirm is an automated identity verification solution designed to ensure that employees and customers are who they claim to be at all times. It provides fast, secure, and passwordless identity verification throughout the user lifecycle.

Key Features of HYPR Affirm:

- **Prevent Identity Fraud:** Utilizes advanced verification technologies to detect and prevent unauthorized access.
- **Simplify and Automate Identity Verification:** Streamlines the verification process, reducing administrative overhead.
- **Continuous Identity Proofing and Verification:** Allows for re-verification at critical moments throughout the user lifecycle.
- **Secure and Accurate Verification Methods:**
    - **Document Verification:** Validates official documents like passports and driver's licenses, detecting any forgeries or alterations.
    - **Facial Recognition:** Employs cutting-edge technology to detect spoofing tactics such as photos or masks.
    - **Location Detection:** Compares geolocation against expected locations while adhering to global regulations.
    - **Chat and Video Verification:** Combines AI and human interaction for secure verification through chat systems and live video feeds.
    - **Manager Attestation:** Allows supervisors to attest to an employee's identity, further strengthening security.

Benefits of Using HYPR Affirm:

- **Enhanced Security:** By eliminating passwords and using biometric authentication, it significantly reduces the risk of phishing attacks and unauthorized access.
- **Improved User Experience:** Offers a fast, intuitive identity verification process that removes user friction.
- **Regulatory Compliance:** Assists in meeting guidelines such as NIST IAL2 and adheres to data privacy laws like PCI DSS, GDPR, and CCPA.
- **Integration Flexibility:** Integrates with various credential systems, including Windows Temporary Access Pass (TAP), and supports a Zero Trust security framework.

What will be the end result of this solution playbook?

After completing this playbook, you will have:

- Defined specific use case(s), where Affirm solves your identity verification business needs
- Established the source of truth for the identity verification user data. Often this is an identity provider such as Okta or Entra, which sources the user data from HR. NOTE: this step may require coordination with other departments within your organization
- Created one or more Affirm verification workflows that implement the business logic
- Outlined a schedule to rollout Affirm to your organization

Getting Started with HYPR Affirm

Generally speaking the best first step(s) for implementing and getting the most out of your investment in HYPR Affirm is to define the current challenges you wish to address through identity verification. The next section provides a template for recording business requirements and documenting any associated questions that may need to be resolved before implementation can be accomplished.

Requirements analysis

Requirement 1 (example)

Statement: Streamline onboarding process for new hire / user

Interpretation: The current business process involves human inspection of a scanned verification document (passport, driver's license, etc.), which is a prerequisite for creating user accounts in the IT system. The business would like to automate verification to improve security and accuracy of new hires. In addition, the user should be able to immediately register for their create their primary authentication account.

Question	Answer

Requirement 2

Statement:

Interpretation:

Question	Answer

Requirement 3

Statement:

Interpretation:

Question	Answer

HYPR Affirm Overview

HYPR Affirm adopts a workflow model for identity verification. Users are given a URL and are guided through a series of steps (screens), in which users are asked to present identifying information. Configuring Affirm as an administrator involves creating a workflow by choosing which verification steps are to be included in the workflow. Once the workflow has been created, Affirm generates a URL to be given to the end user.

Verification Steps

Affirm offers the following verification steps

Name	Description
Login Identifier	Initiates the HYPR Affirm IdV process. This option will always display *Required*.
Escalate to Live Chat	If this feature is toggled On and the requester fails the IdV flow checks, the requester is immediately placed into a video and chat session with the approver.
Phone Number Verification	SMS Code requires the requester to enter an SMS code that is sent to a phone number or email address
Location	A location based upon the requester's IP address will be displayed to the approver.
Identity Verification	This step involves presenting a document (such as

	passport or drivers license) that gets compared against the identity data from HR. It may optionally include a liveness check.
Photo ID and Liveness Capture	Requires upload of a valid photo ID and a subsequent real-time selfie, both of which will be compared to each other to verify a match. This step does not inspect identity data and only concerns image comparison to mitigate risks of deepfakes.
Approver Chat and Video	This step opens a chat window between the approver (often a manager) and the requester.
Attestation	This step is required in order for the workflow to issue an Outcome (i.e. to complete successfully). An approver must review the request before the Outcome is issued. The approver is either a person or HYPR automated approval. HYPR automated approval calculates approval based on the results of the previous steps.
Verified Outcome	What to do after the verification succeeds.
Unverified Outcome	What to do after the verification fails.

Details for each of these steps can be found on the HYPR documentation web site.

Pre-configured Workflows

In order to accelerate the workflow creation process, Affirm offers a number of canned workflows based on business use case and desired friction level. Pre-configured business cases are

- Onboarding - for new hire scenarios
- Recovery Flow - for credential recovery
- CC Admin - for onboarding HYPR Control Center admin accounts

For each of these scenarios, you may choose a friction level. Friction in this case refers to the number of verification steps needed to complete the workflow. There are six levels of friction:

- Highest
- High
- Medium
- Low
- Lowest
- None (no verification steps are pre-selected)

See Appendix A for which verification steps are included in each friction level.

Application assignment

A number of verification scenarios require you to have configured an integration with an Identity Provider (IDP) elsewhere in the HYPR Control Center. IDP integrations allow HYPR to be used as a passwordless authentication mechanism to the IDP. Each IDP integration has an associated application name, often referred to as relying party application (or rpAppId). You will need to have an IDP integration for the following scenarios:

- The selected Verifified Outcome is *Redirect to Device Manager to register a new login method*
- Identity Verification has been selected as a verification step AND you are not using an Advanced Customization to retrieve identity data from an external data source

If one of those two scenarios applies, then you will select the application during the configuration of the Affirm workflow.

See HYPR Integrations for more information on creating an integration.

Advanced settings

There are two types of advanced settings in HYPR Affirm:

1. Customizations - custom code that gets executed during a workflow
2. OIDC Settings - sets up Affirm as an OIDC relying party

These advanced settings provide flexibility for business scenarios that do not fit into the out-of-the-box Affirm workflows.

Customizations

HYPR Affirm allows multiple types of customizations that override the default behavior in key parts of the verification flow. For example, if you need to pull identity data from an external system rather than an IDP integration, then you write Javascript code to retrieve that data as part of the IDV flow.

Types of customizations are

Customization Type	Description
User Directory	This customization allows specification of the user info source.
SMS Sending	Allows sending SMS via a custom REST call instead of HYPR's SMS service
SMS Verifying	Allows handling the result of a verified SMS code through a custom REST call instead of HYPR's SMS service
Email	Allows sending of emails through a custom REST call instead of HYPR's SMTP servers

See Customizations for more details.

OIDC Settings

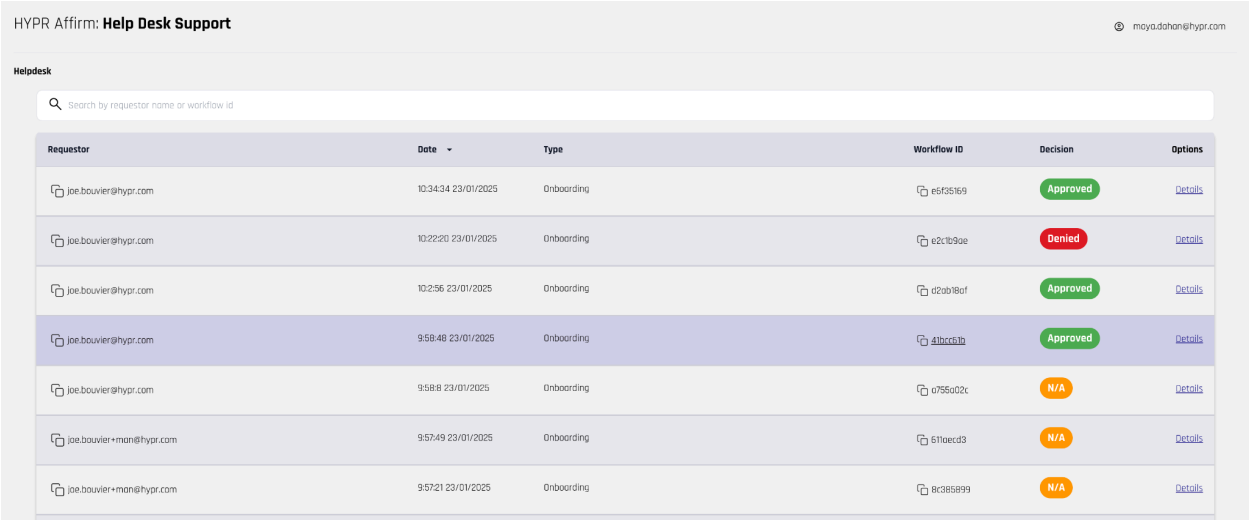
OIDC settings can be used to trigger OIDC authentication for the requester or approver. Currently, these are only assignable to a verification flow via the HYPR Affirm API.

For the requester, this will force an OIDC authentication at the specified part of the flow. It must be assigned to the verification flow, and the setting for the specific step should be enabled to trigger when the authentication should take place.

For the approver, this will force an OIDC authentication before the approver enters a verification flow to which they were invited via email or SMS.

Helpdesk Application (beta in 10.3)

Affirm includes a separate web-based application targeted for Helpdesk operators. For obvious security reasons Helpdesk operators are required to identify the users who call in for support. Oftentimes this includes shared secrets like a PIN or “Secret” questions and answers. The Affirm Helpdesk application relieves the operators of this burden and increases security by reducing social engineering success.



The application displays a list of recent Affirm workflow attempts and the verification results.

HYPR Affirm API

TBD

Solution deployment overview

Affirm is quite simple to configure, but preparation is key to ending up with a solution that meets the business requirements.

You can use the following as a checklist to make sure you cover all the bases:

- ☐ Identify the Affirm verification flow steps that align with your business requirements
- ☐ Determine what the outcome of successful and unsuccessful flows should look like
- ☐ Ensure you have access to the HYPR Control Center
- ☐ Request HYPR deployment team to enable the relevant functionality in your HYPR Control Center (see Appendix B: Feature Flags)
- ☐ Configure your IDP integration or external data source
- ☐ Configure your verification workflow

Solution deployment example

TBD

Configuration Tips and Tricks

IDV failure modes

https://documentation.onfido.com/guide/document-report/#breakdown-descriptions

```
"breakdown": {
   "data_comparison": {
     "result": "consider",
     "breakdown": {
       "first_name": "consider",
       "last_name": "consider"
     }
   },
   "data_validation": {
     "result": "consider",
     "breakdown": {
       "gender": "clear",
       "date_of_birth": "clear",
       "document_numbers": "clear",
       "document_expiration": "consider",
       "expiry_date": "clear",
       "mrz": "",
       "barcode": "consider"
     }
   },
   "image_integrity": {
     "result": "clear",
     "breakdown": {
       "image_quality": "clear",
```

```
      "supported_document": "clear",
      "colour_picture": "clear",
      "conclusive_document_quality": "clear"
    }
  },
  "visual_authenticity": {
    "result": "consider",
    "breakdown": {
      "fonts": "clear",
      "picture_face_integrity": "clear",
      "template": "clear",
      "security_features": "consider",
      "original_document_present": "consider",
      "digital_tampering": "clear",
      "other": "clear",
      "face_detection": "clear"
    }
  },
  "data_consistency": {
    "result": "consider",
    "breakdown": {
      "date_of_expiry": "",
      "document_numbers": "consider",
      "issuing_country": "",
      "document_type": "",
      "date_of_birth": "consider",
      "gender": "",
      "first_name": "consider",
      "nationality": "",
      "last_name": "consider",
      "multiple_data_sources_present": "clear"
    }
  },
  "police_record": {
    "result": "",
    "breakdown": {}
  },
  "compromised_document": {
    "result": "clear",
    "breakdown": {}
  },
  "age_validation": {
    "result": "clear",
    "breakdown": {
      "minimum_accepted_age": "clear"
    }
  },
  "issuing_authority": {
    "result": "",
    "breakdown": {
      "nfc_active_authentication": "",
      "nfc_passive_authentication": ""
    }
  }
}
```

Adding an Integration (Directory Source) to HYPR

HYPR Affirm verifies user attributes such as email, phone number and address from a directory source. There are multiple ways to add a directory source such as through HYPR integration settings or via advanced settings.

Further NOTES on Datasources

For HYPR Affirm to work with the integration fully, the IdP must include the following attributes for all target users:

Username (UPN field for Azure and Username field for Okta)
Email Address

Depending on the specific verification flow configuration, HYPR Affirm requires the following additional attributes:

Mobile Phone Number (Phone Number Verification step)
First and Last Name (Identity Verification step)
Manager Information (Required if Approver type of Manager is set. Manager field for Azure and ManagerId field for Okta)
Street Address (Location step)
City (Location step)
State (Location step)
Postal Code (Location step. This is called Zip code in Okta)
Country Code (Location step)

Adding an Integration (Entra / Okta)

Entra

NOTE - there is configuration on the Entra tenant that needs to be performed, please refer to the following URL for configuration steps:
https://docs.hypr.com/docs/cc/ccInstallCfg/ccInstallCfgIntegrations/ccInstallCfgIntegrationsEntraID/cc-install-cfg-integrations-hypr-enterprise-passkey

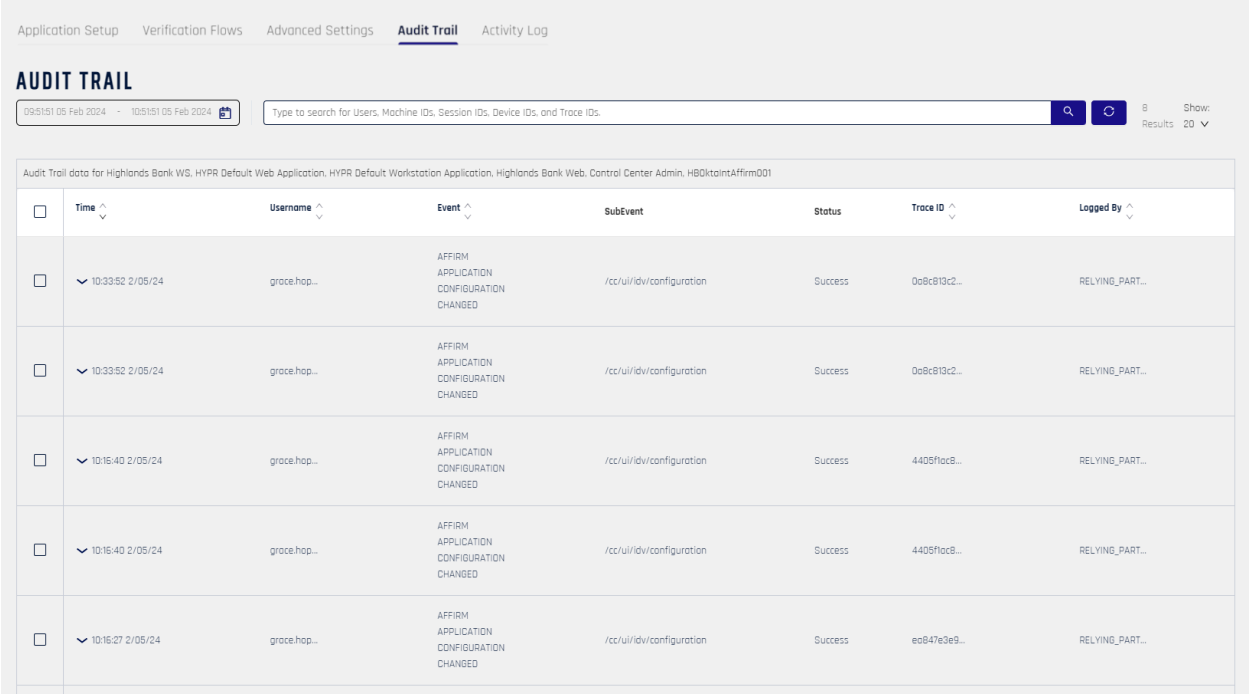
Once the Entra configuration is complete, the integration can be configured.

Analytics Dashboard

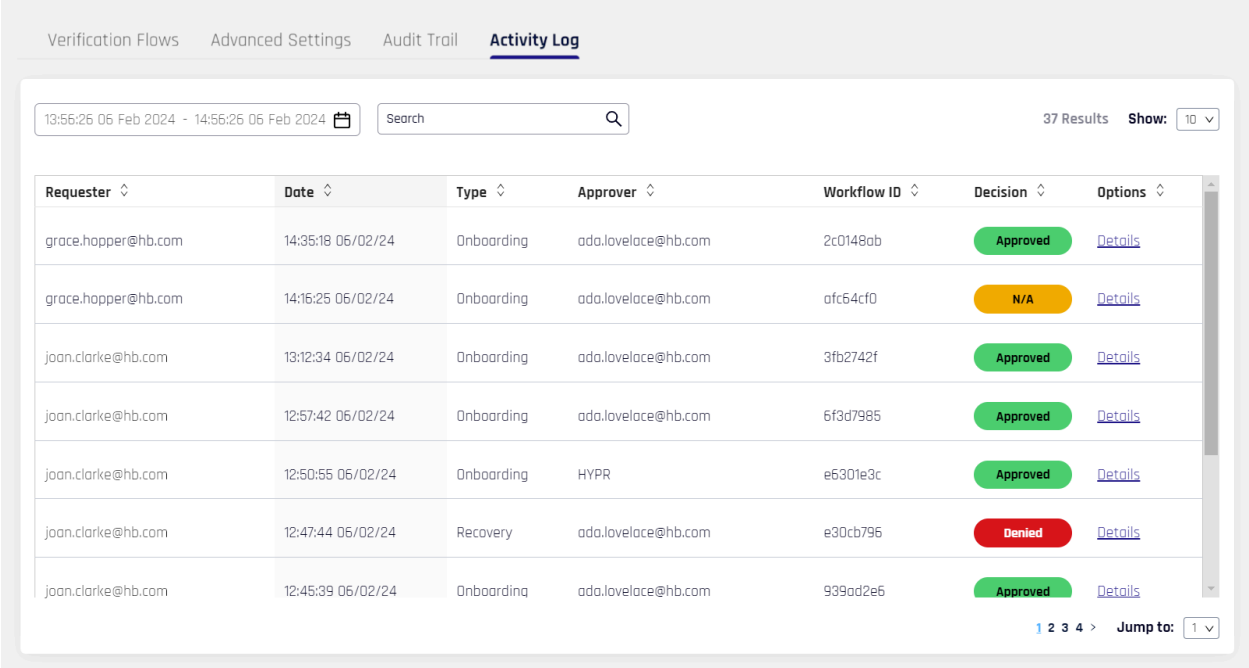
TBD

Audit Trail

HYPR Affirm offers an Audit Trail tab for ease of access. It reflects the Audit Trail experience across HYPR, which is described fully here.



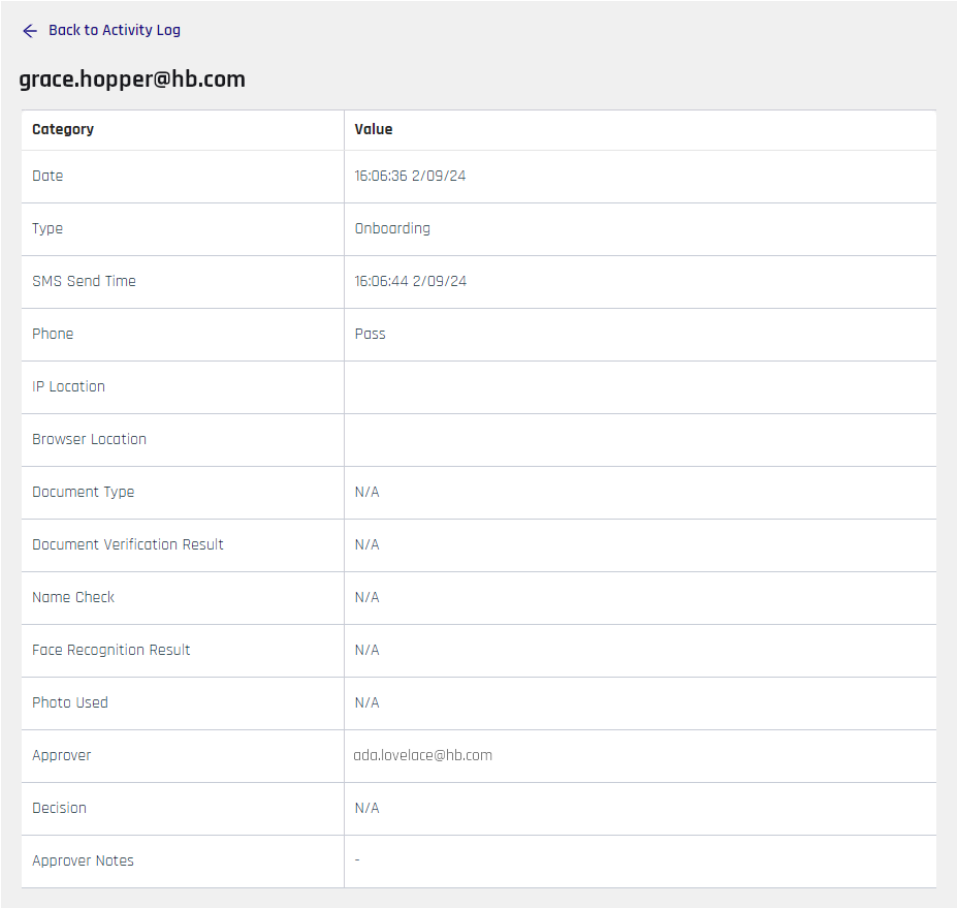
Activity Log



Describe the approved, denied, and aborted attempts to use Affirm. A date selection field and a search bar help filter Activity entries. The *Activity Log* table uses the following columns:

Field	Description

Requester	The HYPR username making the IdV request.
Date	The date and time of the request.
Type	The type of IdV Flow. [`Onboarding` | `Recovery`
Approver	The HYPR username of the approver. If automatic approval is enabled, the *Approver* will be *HYPR*.
Workflow ID	A unique identifier for the request.
Decision	The decision made by the approver. [`Approved` | `Denied` | `N/A`]
Options	Click the *Details* button to display more granular information about the request (see below).



In additional to the main *Activity Log* fields, the following columns are shown on the *Details* page:

Field	Description
SMS Send Time	The time the SMS notification for phone verification was sent.
Phone	Did the phone check pass? *Pass* | *Fail*
IP Location	The local IP address location.
Browser Location	The browser-based location.
Document Type	The type of document uploaded; passport, driver's license, ID card, etc.
Document Verification Result	Did the document check pass? *Pass* | *Fail*
Name Check	Did the name check pass? *Pass* | *Fail*
Face Recognition Result	Did the face recognition check pass? *Pass* | *Fail*
Photo Used	Was a photo used for this request?
Approver Notes	The *comment* for Approvals and the *reason* for Denials.

From the request *Details* page, click *Back to Activity Log* to return to the main page.

Appendix A: Friction Levels

Highest Friction: Includes the highest level of verification steps

Verifications Steps

- Phone Number Verification: ENABLED
  - SMS Code: ENABLED
- Location: ENABLED
- Identity Verification: ENABLED
  - Document Authentication: ENABLED
  - Liveness Check: ENABLED
  - Name Checking: ENABLED
- Photo ID and Liveness Capture: DISABLED
- Approver Chat and Video: ENABLED
- Attestation: ENABLED

Approver Assignments

- Manager Assigned

High Friction: Includes multiple verification steps such

Verifications Steps

- Phone Number Verification: ENABLED
  - SMS Code: ENABLED
- Location: ENABLED
- Identity Verification: DISABLED
  - Document Authentication: DISABLED
  - Liveness Check: DISABLED
  - Name Checking: DISABLED
- Photo ID and Liveness Capture: ENABLED
- Approver Chat and Video: ENABLED
- Attestation: ENABLED

Approver Assignments

- Manager Assigned

Medium Friction: Includes a balanced number of verification steps

Verifications Steps

- Phone Number Verification: ENABLED
  - SMS Code: ENABLED
- Location: ENABLED
- Identity Verification: ENABLED
  - Document Authentication: ENABLED
  - Liveness Check: ENABLED
  - Name Checking: ENABLED
- Photo ID and Liveness Capture: DISABLED
- Approver Chat and Video: DISABLED
- Attestation: DISABLED

Approver Assignments

- HYPR Automated Approver Assigned

Low Friction: Involves minimal verification steps

Verifications Steps

- Phone Number Verification: ENABLED
  - SMS Code: ENABLED
- Location: ENABLED
- Identity Verification: DISABLED
  - Document Authentication: DISABLED
  - Liveness Check: DISABLED
  - Name Checking: DISABLED
- Photo ID and Liveness Capture: ENABLED
- Approver Chat and Video: DISABLED
- Attestation: DISABLED

Approver Assignments

- HYPR Automated Approver Assigned

Lowest Friction: Designed for maximum ease

Verifications Steps

- Phone Number Verification: ENABLED
  - SMS Code: ENABLED
- Location: ENABLED
- Identity Verification: DISABLED
  - Document Authentication: DISABLED
  - Liveness Check: DISABLED
  - Name Checking: DISABLED
- Photo ID and Liveness Capture: DISABLED
- Approver Chat and Video: DISABLED
- Attestation: DISABLED

Approver Assignments

- HYPR Automated Approver Assigned

Appendix B: Affirm Feature Flags

Feature Flags (set by HYPR deployment team)	
Name	**Description**
AFFIRM_PAID	(Required) Enables core Affirm functionality
AFFIRM_CC_ADMIN_ONBOARDING	(Optional) Enable the *CC Admin* workflow Type
ENABLE_AFFIRM_CITRIX_OPTIMIZATION	(Optional) Enables Affirm Citrix media redirection optimization
AFFIRM_AWS_PINPOINT_SMS_V2_API	(Optional) Moves Affirm from using the v1 Pinpoint SMS APIs to the v2 End User Messaging SMS APIs. This is required for supporting sending SMS messages to international users
AFFIRM_HELPDESK_SUPPORT	(Optional) Enables the possibility to allow for helpdesk access & configure helpdesk code to be shown to requestor affirming
AFFIRM_WATCHLIST_STANDARD_ENABLED	(Optional) Allows the watchlist standard checks options to be used depending on Affirm configurations a CC admin is eligible to do

Appendix B: Test Cases

Test ID	Test Case Description	Expected Results	Type	Comment
1	Validate user is successfully able to upload document and take photo with all options	User should be able to complete the verification process with all options	Functional	This scenario will be tested with all 3 options: Scan QR Code, Copy Link, Get link via SMS
2	Validate how system behaves if there is any interruption while performing document upload and photo	User should be displayed with correct error message if there is any interruption or process didn't complete successfully	Functional	Need to check error message description and this scenario will have multiple test case validations

3	Validate time taken by system to validate information after user completed document and photo submission	System should complete verification before 5 min	Non-Functional	Need to check Time SLA
4	Validate e-pass home page is displayed for user after successful completion of verification	E-Pass home Page should be displayed and user should be able to take below actions: Change Passwords, Unlock Accounts	Functional	
5	Validate user is able to login in system using new password after changing the password	User should be able to login with new password	Functional	
6	Validate every page response time when you click on any link while doing the Verify process	Page should be loaded within SLA response time	Non-Functional	Need to check Time SLA
7	Validate how system behaves if verification is failed for user 5-6 times or more	Regulatory/Compliance requirement needs to be checked	Non-Functional	
8	Verify National ID cards document option is not allowed for other work location countries except Canada, China, Germany, India, Moldova, Portugal, Singapore, Serbia, United States, Great Britain, Hong Kong	National ID Cards document should not be allowed for other country work locations except mentioned	Functional	
9	Validate user is provided with 2 options to continue after selecting document: Continue on phone, Upload photo	Continue on phone and Upload photo options should be allowed to user	Functional	
10	Validate user is able to complete the verification processing using "upload photo" option	User should be able to complete the verification process with "Upload Photo" option	Functional	
11	Validate user is able to see button "Get secure link" when continue on phone option is selected by user	Get secure link should be displayed and enabled	Functional	
12	Validate user has below 3 options to get secure link: Scan QR Code, Copy Link, Get link via SMS	Scan QR Code, Copy Link and Get link via SMS should be available for user to get secure link	Functional	

13	Validate Error message is displayed when user enters incorrect mobile number to get secure link	Error message should be displayed when user enters wrong mobile number	Functional	
14	Verify user is able to see and access new option "Login with ID Verification" after providing valid email id	New option "Login with ID Verification" should be available to user	Functional	
15	Validate new option "Login with ID Verification" is Clickable	User should be able to click new option "Login with ID Verification"; HYPR Affirm page should be displayed with user email populated, Begin Button should be enabled	Functional	
16	Verify "Start Verification" button is displayed and enabled on "Verify your identity" page after user clicks on Begin Button	"Start Verification" button should be displayed and enabled	Functional	
17	Verify user is getting an "Issuing Country" dropdown option to select country for submitting document	User should be able to select respective country from dropdown	Functional	
18	Verify IDs allowed to use for document submission	Passport, National ID cards, and Driver's license are allowable documents for user	Functional	
19	Verify National ID cards document option is allowed only for below work locations: Canada, China, Germany, India, Moldova, Portugal, Singapore, Serbia, United States, Great Britain, Hong Kong	National ID Cards document should be allowed only for mentioned country Work Locations	Functional	