Customer Identification Procedures

Date: July 9, 2022

About iComply

iComply is a global compliance software provider that helps compliance teams enhance, improve, and transform their entire client lifecycle management for KYC and AML, while providing a seamless user experience to their KYC subjects.

Table of Contents

The iComplyKYC platform is a digital compliance administrator that leverages edge computing and AI to provide companies with dynamic, guided KYC portals. Compliance teams can configure and monitor portal workflows to securely gather, validate, and encrypt client data and documentation before it leaves their device.

Document Overview

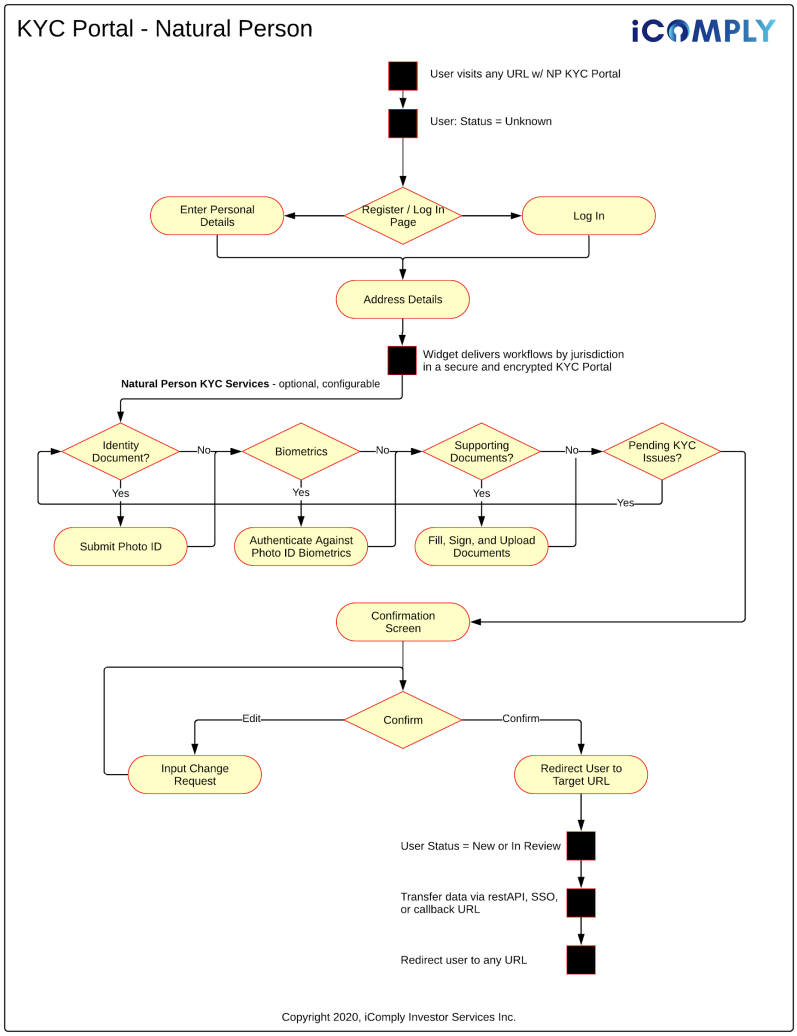
This document outlines the manner in which entities are identified and the steps involved in the compliance process(es) provided by iComply. The iComply platform is fully modular meaning that any of the following modules may be used independently or in a workflow configuration of multiple modules. Each workflow is deployed as an encrypted and secure portal to gather, authenticate, and verify entity information for the purposes of KYC documentation, AML screening, and regulatory reporting purposes.

Third party services may be utilized in a streamlined workflow to perform each step. Depending on your configuration these services can be provided by iComply, our partners, or you may integrate your own preferred vendors (KYC Enterprise licenses only).

Process Description for Natural Persons

The following modules can be deployed via the iComply portal and used for the purpose of verifying, authenticating, and documenting the identity of a user in a non-face-to-face environment:

- Use Onboarding
- Document Authentication
- Identity Data Verification
- Biometric Authentication
- Liveness Detection
- Live Face Matching
- Supporting Documents
- Enhanced Due Diligence



User Onboarding

The user onboarding module can be delivered as a web form within your portal (for scenarios such as user onboarding) or can be passed directly into the portal (using an API or similar technical solution). All data submitted via either method is prescreened and then encrypted within the portal before being sent to a server to begin third party verification workflows.

Via Web Form

1. User uses a web form embedded in your website and enters their personal information and address details. The data collected is as follows:

Personal Information	Address Details
Given Name	Street Address
Middle Name	Unit/Apt
Surname	City
Date of Birth	Country
Email	State/Province
Phone Number	Zip/Postal Code

2. The web form contains logic for data validation, bot detection, cyber-fraud monitoring, and preliminary user screening (i.e. jurisdiction, age, digital fingerprints).
3. Additional hardware, software, behavioural, geolocation, and connectivity information (i.e. IP Address), may also be collected for fraud detection purposes.

Via API

1. User data is passed directly into the iComply portal and is encrypted prior to leaving the user's device.
2. You have the option to use the data to prepopulate the Web Form in the portal (i.e. to have the user confirm data accuracy), or bypass the Web Form entirely and move the user into the next step of the workflow.

Via API + Webform

1. The user's current data is passed into the web form via API to prepopulate fields for Personal and Address Information.
2. The user is able to review, edit, and submit the data populated into the web forms.
3. This feature is best suited for applications where the user may need to correct or update their KYC data.

Identity Document Authentication

The document authentication process is designed to detect fraud, validate document authenticity, and verify user information such as name, address, date of birth, jurisdiction of domicile, among others. The process is split into two stages; authentication which - in jurisdictions where possible - is largely performed on the user's device, and verification which can involve third party services and data sources including the applicable government for that user.

This comprehensive process includes a suite of high performing technologies configured into a series of steps including:

1. The User selects a supported document type and then uploads an identity document into the portal. Please see the **Document Authentication Coverage** list for details on supported documents by jurisdiction.
2. Based on the user's jurisdiction, a range/set of document files will be loaded into the portal and used to authenticate the User's document.
3. Depending on the type of document used for verification, either one or both sides of the document may be required (i.e. one side is required for a passport whereas a driver's license or government issued ID card typically requires both sides).
4. Machine Vision Technology is first used to determine if the document image is viable (blur, glare, fingers in front of text, barcodes, security features, etc).
5. Machine Vision Technology is then used to analyze the document for the presence of security features, detect potentially fraudulent documents, read the MRZ or barcode, and confirm a match to the corresponding identity document validation file.
6. Optical Character Recognition (OCR) technology is then used to read the data from the identity document and perform the following checks:
    a. MRZ or barcode data match;
    b. User onboarding data match.
7. If any errors occur, the failure is logged and the user may be required to submit additional photos of their identity document, upload additional supporting documents, or enhanced screening during the identity verification process.
8. If the document undergoing authentication includes an image of the identified individual, the image is extracted from the document, encrypted, and held for analysis during the identity verification and facial matching processes.
9. Once the document authentication process is complete the user data, test data, and data hashes are encrypted and securely stored* on the iComply platform in accordance with the client's data retention requirements.
   **Client's may provide their own servers to store their user data, speak to your account manager for more information.*
10. In some configurations, such as where document verification may be required, the document image may then be sent to a qualified third party for matching or verification

against a government-issued identity document template, government agency database(s), or trusted and approved service provider.

Identity Verification

A digital identity verification is a process used by computer systems to represent a unique person, organization, application or device. So for a natural person or legal entity, a “digital identity” is a trusted way of validating one or more attributes about the client, either online or offline, and then linking those validated attributes to a uniquely identifiable client. The identity verification process can change significantly by jurisdiction.

iComply’s primary sources for validating uniquely identifiable attributes are public data records. In our experience, identity verification services that rely solely on credit data have lower match rates and expose clients to significant privacy and technology risks such as the massive data breaches that frequently occur at these same credit agencies. However, in many jurisdictions, there may be legislated requirements to use data provided from credit headers, utilities, or mobile communications providers. In these cases, iComply uses qualified third parties with the appropriate licenses and current cyber-security certifications to validate attributes solely for the purposes of digital identity verification.

Our data sources include more than 33 billion records and tens of thousands of resources and data is updated on monthly, daily, hourly, or near real-time maintenance cycles. We access a wide variety of data sources to meet the varying requirements across jurisdictions on a real-time basis including:

Corporate Registries	Reverse Lookup	Professional Licenses	DEA CS License
Bankruptcy	Mobile Providers	Property Assessment	FAA Aircraft Registry
Driver’s License	Civil Court Filings	Credit Headers	FAA Pilot License
Geolocation	Motor Vehicle Registries	Concealed Weapons Permit	Firearms & Explosives License
Subscriber Identity Modules	Hunting/Fishing License	Voter Registration	Property Deed Search
Directory Assistance	Person Search	Criminal Conviction	Accident Registries
Internet Domain Name	Merchant Vessels	UCC Filings	Companies House

Biometric Authentication

iComply supports two methods in order to complete a Biometric Authentication using Facial Matching; Live Face Match or Selfie Upload.

While the selfie upload is typically faster and more convenient for the user, it also represents inherent weakness to fraud including manipulated images, stolen images (such as publicly available images from the individuals social media profiles), deep fake images, and more.

On the other hand, Live Face Match can take longer, requires the user to have access to supported hardware and software, but can easily be used to prove that the user behind the screen is the same user whose identity is being authenticated, validated, or reverified.

The system administrator can configure settings for Biometric Authentication including:

- Biometric Facial Match Confidence and Sensitivity
- Liveness Confidence and Sensitivity
- Auto-Acceptance for straight through processing where no potential issues are identified
- Auto-Assignment for escalations where potential issues are identified

Facial Matching

Facial matching is the process of comparing an image submitted by the user to the photo on their authenticated government-issued identity document. In many jurisdictions, facial matching is still not an explicit requirement for customer identification. However, in most of these same jurisdictions, there are requirements that a risk based approach be applied and that a strong client authentication program is easy to demonstrate, audit, and review. In our experience, the facial matching process is a minimum requirement to ensure that the user behind the screen is the same user whose identity documents are being authenticated.

Depending on your workflow configuration, the user can be directed through either the Live Face Match or Selfie Upload workflows in order to complete the Biometric Authentication processes.

Liveness Detection

Liveness detection is the process of ensuring that the user behind the screen is a living person by analyzing the user's camera feed to confirm movement. There is a wide range of variability in how Liveness is performed including "blink detection", other types of motion detection, and gesture detection.

Processes that employ blink or motion detection are inherently weak as they only are capable of verifying basic information. For example, blink detection focuses on tracking the user's face, locating their eyes by searching for the whites of their eyes, and then waiting to see if the whites of their eyes disappear - such as when they blink. Often, these processes can easily be cheated by simply taking a photo of the KYC subject, such as the one found on their identity document, holding it in front of the camera, and briefly covering the whites of the eyes in the photo.

Due to these vulnerabilities, iComply employs a combination of edge computing and machine vision techniques to generate a Live Face Match which includes a randomized series of liveness

tests. Randomization is based on the number and type of tests activated in the system, such as detecting facial expressions: Neutral, Smile, Frown, Angry, Surprised.

Live Face Match

The Live Face Match module directly accesses the user's camera hardware on their device to check in real time if the user being identified is present, assess for deep fakes, detect fraud and suspicious behavior, and interact with the user to perform a facial match against the biometrics extracted from their identity documents, or if enabled, biometrics on file.

1. The User begins a Live Face Match by activating the feed in the portal and allowing the program access to their camera.
2. Once initiated, the user is requested to look at the camera with a neutral facial expression to form a facial recognition baseline.
3. A unique test program is assembled for every User journey based on the User's jurisdiction, hardware, software, workflow configurations, and test order are randomized enabling hundreds of thousands of possible configurations.
4. The test program is then encrypted and sent to the User's device to ensure the test is performed in the same jurisdiction the User's device is currently in.
5. Once a neutral facial expression is detected the program will simultaneously execute a battery of tests including:
6. A series of facial expressions and gestures are randomly selected, ordered, and delivered to the user from iComply's library of Liveness tests. The purpose of this test is to keep the user interacting long enough to ensure the highest degree of integrity in the test.
7. As the User interacts with the program, a unique biometric file is created based on the way their face moves (not a facial vector). This file is impossible to trace back to the user (i.e. reverse image search) as it is not an image file, the only way to recreate this file is for the same person to agree to successfully reverify using the same program.
8. As the User interacts with the program, machine vision is used to continuously identify and track the User's face, assess whether other faces that may appear in the video stream, and match the User's face to the image extracted from their identity document.
9. As the User interacts with the program, a photo or series of photos may be captured for future auditability - depending on your configuration.
10. As the User interacts with the program, a series of fraud detection measures analyze the feed to detect bots, spoofing, and deep fakes.
11. Device connectivity and attempts to manipulate the camera hardware are monitored, if present the test will fail and the error logged.
12. Once the unique test program has successfully completed the data is encrypted on the device, hashed, and the data*, test data, and data hashes are encrypted and securely stored** on the iComply platform in accordance with the client's data retention requirements.
    **Client's may provide their own servers to store their user data, speak to your account manager for more information.*

***Client's may configure the portal to send data directly from the user's device to their own server, eliminating the need for user data to be sent to an iComply server.*

13. Should the User's hardware or software not support live face matching, or should the program fail to initialize, the User will be directed to the Selfie Upload alternative.
14. Should the program fail or appear to be interrupted or corrupted during the test, the User will be directed to restart the process.

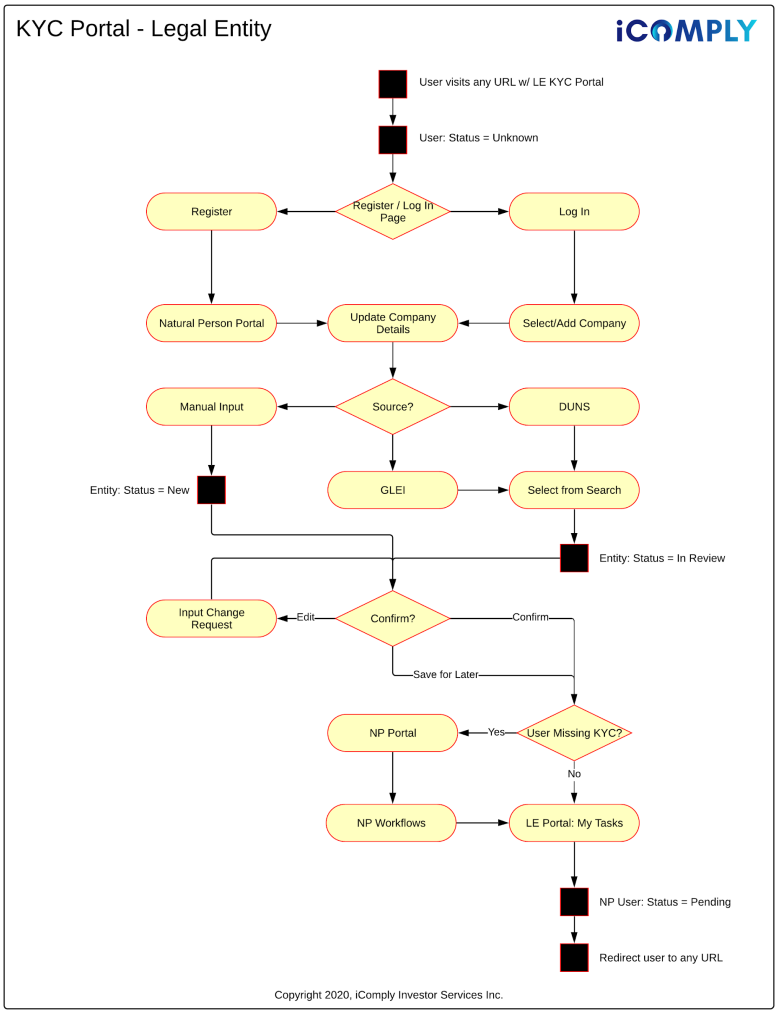
Selfie Upload

1. The user is directed to upload a file from their device or capture a "selfie" photo using the camera on their device.
2. A facial matching program is loaded into the User's device to perform the test on their device. This improves fraud detection measures and the user's experience. The program executes a series of tests:
3. The image is analyzed for potential fraud, media manipulation, and to ensure the image is viable.
4. Machine vision is used to compare the face in the selfie against the photo extracted from the identity document submitted for validation.
5. If problems are detected, the user may be requested to upload an additional image or may be required to capture an image only.
6. Once the unique test program has successfully completed the data is encrypted, hashed, and the data, test data, and data hashes are encrypted and securely stored* on the iComply platform in accordance with the client's data retention requirements. These are versioned to provide a compliance audit trail around future verifications (ie. in the case of an expired identity document).
   **Client's may provide their own servers to store their user data, speak to your account manager for more information.*

Process Description for Legal Entities

The following modules can be deployed via the iComply portal for Legal Entities and used for the purposes of authentication, onboarding, and screening users globally as individuals or authorized representatives of legal entities. Secure and encrypted KYC Portals support unique regulatory workflows for all ISO-3166 jurisdictions. Legal Entity Portals enable:

- Nominee Identification
- Legal Entity Onboarding
- DUNS
- GLEI
- Legal Entity Verification
- Legal Entity Investigation
- Beneficial Ownership
- Power & Control
- Supporting Documents
- Enhanced Due Diligence
- Attorney Confirmation
- Agent Submissions



Nominee Identification

In order to verify the identity of the nominee the user will be directed to the URL that hosts the KYC Portal for Natural Persons. The user will be asked to submit KYC data and documents for onboarding, authentication, and verification according to the unique jurisdictional workflow configurations as outlined in the Process Description for Natural Persons.

Legal Entity Onboarding

Once a portal user has been successfully identified, they will be able to complete Legal Entity Onboarding as a verified user. While it is possible to configure the system to support the onboarding of Legal Entities with unverified users, it is not recommended as this tends to lead to higher rates of fraud, bad data, and increased costs.

iComply supports three methods of onboarding legal entities: DUNS, GLEI, and manual entry. Depending on the system configuration, the LE Portal can support any or all of these methods.

DUNS & GLEI

Where a DUNS or GLEI process is used, the portal user is able to search by the legal entity name, address, and DUNS or GLEI numbers. The portal user will be able to select their company from the search results, review legal entity details, and provide updated key information such as address and contact information. Once submitted through the LE Portal, the legal entity data will be visible in the KYC Dashboard.

Manual Entry

When using the manual entry method, a portal user will be able to enter legal entity information, review, and confirm their submission. No validation is performed at the submission stage. Once submitted through the portal, the legal entity data will be visible in the KYC Dashboard. In the KYC Dashboard, users may review, update, approve or reject the submission, or initiate a Legal Entity Verification request on the legal entity.

Legal Entity Verification

Identity verification on legal entities can be completed almost instantly when sufficient data is available - such as when the legal entity has a valid DUNS or GLEI file. For private companies, the DUNS or GLEI data is often stale, or may not exist at all. In these cases, an Investigation into the company can be initiated to confirm the identity of the legal entity, and update or create a legal entity identifier.

Legal Entity Investigation

Investigations can include tasks such as authenticating authorized contacts, directors & officers, addresses, proof of incorporation, and proof of residency. A request for a Legal Entity Verification can be submitted in the dashboard, through workflow automation, or via the API.

Legal Entity Addresses

Address verification may require supporting documentation, biometric authentication, and manual processing. Authorized representatives of a legal entity are able to update their primary and secondary addresses through the Legal Entity Portal.

Address information can be validated against third party data sources such as DUNS and GLEI for automated processing. In exceptions where straight-through processing is not possible, the Issue will appear in the KYC Dashboard for manual review and approval.

Nominee Authorization

Once a user has completed has been successfully identified and approved as a natural person, they will be able to submit data about a legal entity for identity and address verifications. Nominee authorization confirms that the identified natural person is authorized by the legal entity to represent the legal entity.

Nominee authorizations can be performed by matching the identity of the user to a primary contact, director, officer, or authorized representative of the legal entity. Straight-through processing can be configured but exceptions will still appear in the KYC Dashboard as Issues. Enhanced workflows can trigger Supporting Documents and Enhanced Due Diligence requests to the Legal Entity Portal while the user is still in session.

Beneficial Ownership

Entity relationships can be linked in the KYC Dashboard to show beneficiaries above set thresholds of ownership or control. Enhanced Due Diligence workflows can be configured to accept Supporting Documents through the Legal Entity Portal.

A Beneficial Ownership request will compare the current list of beneficiaries against third party data sources, such as DUNS or GLEI. Straight-through processing can be configured to allow direct matches, while Enhanced Due Diligence workflows can trigger a request for an Investigation or Support Documents request.

Ultimate Beneficial Ownership

In many cases, the list of Beneficial Owners can include legal entities, such as companies, trusts, organizations, etc.. Ultimate Beneficial Ownership reviews can be managed in the KYC Dashboard by initiating Beneficial Ownership reviews on all entities listed that are not Natural Persons. Enhanced Due Diligence workflows allow straight-through processing on direct matches or trigger a new request for an Investigation or Support Documents.

Supporting Documents

Throughout the KYC customer lifecycle, Supporting Documents are frequently required to verify identities, addresses, beneficiaries, tax residence, credit worthiness, etc. Supporting Documents can be added to unique workflows varying by industry, jurisdiction, risk level, or KYC Portal.

Requests for Supporting Documents can be triggered by the KYC Subject while they are in the Legal Entity and Natural Person Portals, they can also be triggered through the KYC Dashboard or iComply API.

Enhanced Due Diligence

Enhanced Due Diligence workflows are frequently required in day-to-day user onboarding, KYC reviews, and annual tax or financial reporting. Thresholds and triggers can be configured to request Supporting Documents and other KYC Services such as Identity Verification, Beneficial Ownership, or Third-Party confirmations.

The KYC Dashboard enables users to review pending requests, submit additional requests, and manually upload submissions for cases where a KYC subject has submitted the information through another channel, such as unsecured email.

The KYC Portals actively monitor the data submitted by the KYC Subject to assess for Enhanced Due Diligence thresholds. If a threshold is crossed, such as if the user is required to supply two pieces of address information in their jurisdiction, the additional KYC Request is triggered - in this case, the user could be presented with a web form to upload a recent bank statement or utility bill that shows their address.

Additional KYC Services can also be triggered by Enhanced Due Diligence thresholds. Jurisdictionally specific workflows can enable variations such as the percentage of ownership required for a Beneficial Ownership request.

Third-Party Representatives

**This is a beta feature, contact your account manager for details.*

Legal counsel, nominees, and powers of attorney are examples of third party representatives that can be Authorized to submit information on behalf of a legal entity.

In jurisdictions where straight-through processing is not possible, whether to regulation or market availability, third party representatives such as legal counsel become an integral part of the KYC customer lifecycle.

Configure Enhanced Due Diligence workflows to include a review by the legal entity's legal counsel or board of directors. Authorized representatives can review and confirm the information submitted by their clients for:

- Beneficial Ownership
- Regulatory Reporting
- Financial Records
- Board Resolutions
- Annual Filings
- Tax Reporting