Jumio Solution for TCS BaNCS Customers

Overview of Jumio Services

Leveraging powerful technology including automation, biometrics, AI/machine learning, liveness detection and no-code orchestration with hundreds of data sources, Jumio helps you fight fraud and financial crime, onboard good customers faster and meet regulatory compliance including Know Your Customer (KYC).

The Jumio platform provides services that verify the identities of new and existing users, assess risk, and detect fraud while meeting compliance mandates. TCS has pre-integrated Jumio IDV services into the TCS BaNCS digital banking platform and customers can utilize Jumio to achieve the following:

- **Onboarding** — Establish Trust from the Start: Deter fraud and assess the risk of new customers in real time with identity verification and risk signals
- **Ongoing Authentication**— Maintain Trust Along the Way: Keep your business safe and compliant through biometric authentication.
- **Orchestration** — Streamline the Trust Experience: Build powerful, risk-based workflows for your exact business needs with our orchestration layer while providing a great end-user experience

The Jumio platform provides customizable and flexible workflow capabilities. This allows orchestration workflows to include access to one or more of Jumio's products and selected third-party partner products. With the Jumio platform, TCS BaNCS Customers can create dynamic workflows that trigger the right assessments at the right time, creating friction only for high-risk individuals. TCS BaNCS Customers can utilize our expert-built library of rules and use the intuitive rules editor to customize them, review high-risk transactions with our intuitive case manager, and adjust your rules in real-time with the self-service rules editor. Key capabilities of Jumio's platform include:

- Unified API access to Jumio's products and certified third-party services.
- Orchestration workflows that output identity verification tailored to unique business needs.
- Self-service rules editor for implementing custom risk-based decision logic.
- User-friendly dashboard providing visibility into detailed analytics.
- Seamless integration of Jumio's Identity Verification process and optional Risk Signals allows TCS BaNCS Customers to establish the user's identity and assess their risk in a single step.

Jumio provides an aggregated risk score to TCS BaNCS Customers with reasoning as to why the risk score is what it is. We integrate with hundreds of data sources and can verify thousands of ID types quickly and accurately, all from a single integration point. Our customers can easily create advanced workflows using our no-code orchestration layer to suit their exact business requirements and perform additional checks only as needed based on the risk signals that are returned in real-time. This makes it simple for you to take a risk-based approach and comply with regulatory requirements without sacrificing customer experience.

Identity Verification

Jumio Identity verification will help TCS BaNCS Customers to know the true identity of your applicant drivers by capturing a picture of their ID document and a corroborating selfie. Jumio Identity Verification uses AI, machine learning, and face-based biometrics to ensure the person behind a transaction is present and who they say they are. Because Jumio Identity verification pairs a government-issued ID with a selfie (and built-in liveness detection), it delivers a powerful fraud deterrent to cybercriminals. It has a significantly higher level of identity assurance.

Every government-issued identity document (ID) — whether it's a driver's license, identity card, or passport — has a specification that defines the layout of the document, the relative position of specified fields, labels and images, font types, color, size, spacing, and patterns. Every ID also contains a unique set of security features such as a ghost image, watermarks, holograms, microprint, chip, and machine-readable zones. These features can vary from state to state and country to country. We use these details to auto-detect and classify the document type.

Document Templates
Government-issued IDs (driver's licenses, passports, etc.) follow strict templates defining layout, fonts, and security features (holograms, microprint). Jumio leverages these design elements to ensure authenticity, combat fraud, and prevent unauthorized access by bad actors. Nevertheless, Jumio goes beyond visual inspection to ensure document authenticity. We take a multi-layered approach to fraud detection and leverage cutting-edge technology, as highlighted at https://www.jumio.com/technology/#fraud_detection and in the subsequent sections of this proposal.

Jumio performs a variety of AI-driven fraud checks on these ID documents to ensure that the submitted ID conforms to these government templates and does not exhibit signs of fraudulent tampering, such as text and photo manipulation. Using informed AI, our advanced machine learning models can detect sophisticated attacks that are undetectable by the human eye.

Specific attributes validation include:

- MRZ and HRZ checks
- Ghost image comparison
- Front & back mismatch
- Photo manipulation
- Expired/Invalid ID checks
- Digital copy detection
- Document layout
- Repeated fraud detection
- RFID (NFC) chip detection
- Data validation and syntax checks
- Image manipulation
- Photocopy or Black-and-white detection
- Microprint detection
- Perforation detection
- Deepfake image check

The verification process also includes matching the ID document images against a fraudulent database and the internet in real-time, i.e., an image search. This will identify where ID documents are in the public domain and potentially fake, stolen, or at risk.

Our proprietary ID Verification solution includes a document template (Document Assembly Object, or DAO), which comprehensively details all relevant information about a document. This information includes direct checks that come from the document issuer and derived checks that are defined by Jumio. Direct checks include issuer-defined security features, the fields that need to be extracted, and the rules that need to be applied to the fields. Jumio's derived checks include items like comparing the age estimated from the user's selfie with the DOB and date of issue. All these templates are stored in a Document Database (DDB). The Document Assembly Objects are created manually by a dedicated team of document experts based on document specifications from the issuers like AAMVA and the team's own research. Whenever we encounter a new document type that is not yet in the DDB, we create a new DAO and populate the required values. We have a tool that facilitates the team in creating and maintaining these templates very efficiently.

Jumio's Identity Proofing Process

Jumio's typical identity verification workflow comprises the following steps:

- **Acquisition** (Web, Mobile, or API): The process of getting the images/frames of the document from the end user
- **Image Quality Checks**: This is the process of assessing whether the quality of the images is sufficiently good. It includes instant feedback to increase conversion.
- **Data Extraction**: The process of extracting textual information from the document, utilizing all sources (HRZ/MRZ/barcode/QR)
- **Fraud and Risk Checks**: The process of executing all the fraud checks, which includes the visual inspection, checking security features, checking for typical fraud attacks, and comparing the different data points extracted in the different extraction methods
- **Selfie + Liveness Detection**: In this stage, Jumio performs fully automated face matching and liveness detection. To include:
    a. Compares biometric selfies against ID photos and verifies liveness.
    b. Detects deep fakes, selfie age, date of birth mismatch, and more.
    c. Includes instant feedback to increase conversion.
- **Response and Storage**: Returning the callback to the customer and storage of images + all results of each processing step

The individual steps are executed in parallel whenever possible. This workflow is highly customizable — individual checks can be switched on and off for an account, and thresholds can also be set on an account level.

Biometric Verification

Selfie Verification

We perform a facial biometric similarity check, which establishes that the user uploading the ID is the same person pictured on the ID document. The online user must take a selfie matching the photo on the ID document during this step. Jumio's facial matching technology automatically compares the photo ID and selfie, and a match is verified.

We also verify "liveness," confirming a human being is present, not just a manipulated image. This goes a step further by detecting sophisticated deepfakes, those eerily realistic synthetic videos. We also analyze selfie age and compare it to the date of birth listed on the ID, catching any potential discrepancies. During the process, Jumio provides instant feedback, streamlining the verification process and significantly boosting conversion rates.

Liveness Detection

Whereas facial recognition can accurately match facial similarity, it is equally crucial to ensure that the online user is physically present during the transaction and also check whether it is, in fact, a natural person.

Jumio’s liveness detection is ISO 30107-3/NIST-compliant and provides assurance that users who have completed the onboarding process are legitimate human beings who are physically present during transactions. It examines biometric data for signs of presentation attacks, including attempts to deceive the system with manipulated selfies, and paper or screen-based attacks, among others. Additionally, this technology ensures that the video stream being captured is live and not pre-recorded, making it difficult for attackers to use deep fake videos to bypass the system.
Jumio liveness detection has passed Levels 1 and 2 testing by NIST/NVLAP Accredited Lab iBeta for ISO Presentation Attack Detection and has been extensively tested by third-party organizations, including national governments.

Instant Feedback

Jumio’s solution also guides users through the capture process step-by-step and provides real-time feedback to ensure that the images are clear and of quality. We refer to this feature as instant feedback (e.g., too dark, too light, too blurry) to help users optimize the image capture process. Through Jumio's instant feedback, end-users are guided to provide quality images during each step of the user journey, giving them more granular feedback and the ability to provide a new image immediately. With this service, end-users have a second chance to recapture the image and effectively course-correct for the mobile and web acquisition channels. Where images are submitted without course-correct, i.e., by AP (see section 5.1 for more information about integration channels), Jumio returns specific and highly actionable rejection reasons that enable our clients' users to correct, address the reason for failure, and retake a picture of their ID.

Jumio DOCProof - Non photo ID Document Proofing

Our optional DOCProof document verification solution enables the scanning of various types of other documents such as utility bills and bank statements and supporting data extraction of key data from those documents. This typically supports the core IDV solution and offers a means to verify recent address details as required by many regulatory authorities.

This is principally a document capture and data extraction service though it can be overlaid with a level of forensic document inspection to identify signs of manipulation. We are typically dealing with unstructured data from a vast array of possible documents. The data extracted differs by document type and we typically work with customers to refine exact requirements., We can support documents from every official country with a three letter ISO code. The principal requirement is that the document is in a latin based alphabet for data extraction.

The types of document supported it is possible to support dependent on specific country include:

- BC (Birth certificate)
- BS (Bank statement)
- CAAP (Cash advance application)
- CB (Council bill)
- CC (Credit card)
- CCS (Credit card statement)
- CRC (Corporate resolution certificate)
- HCC (Health care card)
- IC (Insurance card)
- LAG (Lease agreement)
- LOAP (Loan application)
- MEDC (Medicare card)
- MOAP (Mortgage application)
- PB (Phone bill)
- SEL (School enrolment letter)
- SENC (Seniors card)
- SS (Superannuation statement)
- SSC (Social security card)
- STUC (Student card)
- TAC (Trade association card)
- TR (Tax return)
- UB (Utility bill)
- VC (Voided check)
- VT (Vehicle title)
- WWCC (Working with children check)
- CUSTOM (Custom document type)

Jumio Service Architecture

Jumio is a public cloud based service only and cannot be deployed on site or to other cloud infrastructure apart from long term data storage.

Jumio uses AWS for infrastructure services. The Data centres are strategically located in US, Europe and Asia to serve our three key theatres of operation: NA and LATAM, EMEA and APAX. Data centres are based in N. Virginia, N. California, Dublin, Frankfurt (DR) Singapore and Sydney (DR).

Security

Jumio implements stringent security control measures to protect its sensitive data and systems. These controls can be categorised by type (i.e., technical, administrative, and physical) and function (i.e., preventive, detective, corrective, compensatory, or deterrent).
Jumio's security control types

1. Administrative controls: These security measures refer to policies, procedures, or guidelines that define personnel or business practices consistent with Jumio's security goals. These are applied to employee "Joiners, Movers, and Leavers' ' processes, equipment access and internet usage policies, physical access to facilities, separation of duties, the principle of least privilege and need-to-know basis, data classification, and auditing. Security awareness training for employees also falls under the umbrella of administrative controls.
2. Physical security: These are the means and devices that Jumio utilises to control, prevent, or detect physical access to Personal Data. Physical controls include but are not limited to guards, biometric access controls, CCTVs, and environmental controls.
3. Technical security (also known as operational or logical controls) covers technological systems, hardware, or software, used to protect Personal Data. These include encryption, authentication, intrusion detection, and protection systems (IDS/IPS)

Control functions

1. Preventive controls attempt to prevent an incident from occurring.
2. Detective controls attempt to detect incidents after they have occurred.
3. Corrective controls attempt to reverse the impact of an incident.
4. Deterrent controls attempt to discourage individuals from causing an incident.
5. Compensating controls are alternative controls used when a primary control is not feasible.
6. Controls are also used to protect people, as is the case with social engineering awareness training or policies.

Data in transit protection

Customer data is encrypted in transit using TLSv**1.2** and/or above.
We also have **ALE** (application layer encryption/end-to-end encryption) underneath TLS for payload encryption to ensure maximum data protection.
At rest via **AWS KMS** in combination with block storage encryption, selected data is encrypted on a field level using **AES-256**

Compliance with cyber security policies, standards – Cyber essentials +, ISO27001

Compliant with GDPR

Complaint with SOC 2

Compliant with NIST LEVEL 2

We have a comprehensive vendor review process that is approved by management and independently audited regularly as part of our SOC 2, ISO 27001 and PCI certifications. The reviews are performed by our GRC (Governance, Risk and Compliance) team. We do not share the details of the review, but can state that the review was last completed in July 2022 and the vendor is scheduled to be re-assessed in July 2023
Jumio has a formal information security program to manage data security. It consists of a comprehensive and documented set of policies, procedures, guidelines, and standards to protect the confidentiality, integrity, and availability of all the sensitive data across the organisation.
Jumio's information security program is aligned with PCI-DSS and ISO 27001 industry standards

Human Verification

Whilst most of Jumios services are delivered in a fully automated mode where our optional enterprise solution is used (fallback from full automation to human review) then Jumio's Verification Experts are based out of our subsidiary office in India. They are all trained by Jumio.mJumio's Amazon WorkSpaces solution enables agents to perform verification transactions within a secure, isolated remote desktop environment.

Jumio Support and Maintenance

Jumio's Global Support Centers provide our customers with 24/7 support services via our support website, phone or email. Our account managers and technical support engineers have vast experience across multiple IT disciplines, as well as a background in network engineering and operating systems, which allows them to quickly and accurately answer your technical inquiries. We utilise a follow-the-sun, always-available support model. Please see our support datasheet for further information.

Jumio utilizes a follow the sun support model operating from US, EMEA and Indian base offices. Support operatives will have managed and monitored access to customer data not deleted from Jumio servers, this is solely for the purposes of providing support. Support agents view cases and data through Jumio's secure Desktop-as-a-Service (DaaS) solution.teslaapple