CUSTIE PLATFORM

KYC/KYB Identity Verification & Underwriting Policy

Fraud Operations & Trust and Safety

Confidential | Internal Use Only

Document Owner	Fraud Operations & Trust and Safety
Classification	Confidential - Internal Use Only
Applies To	All participants seeking access to the Custie platform

1. Purpose & Scope

This document defines the Know Your Customer (KYC) and Know Your Business (KYB) identity verification and underwriting procedures governing participant onboarding onto the Custie platform. Custie is a B2B/B2C platform connecting pet-care service providers with pet owners. This policy applies to all individuals and businesses seeking access to the platform.

The purpose of this policy is to:

- Establish a structured, repeatable onboarding and verification process
- Prevent fraudulent, misrepresented, or bad-faith participants from accessing the platform
- Protect the integrity of the platform community and the safety of end consumers
- Ensure all participant data is collected, stored, and reviewed in a consistent and defensible manner
- Define clear decision criteria for the approval and rejection of onboarding applications

This policy is designed and operationalized without the use of third-party fraud tooling. All verification, review, and decision-making processes are executed through Custie's proprietary internal admin portal, built and hosted on AWS.

2. Participant Classification

The Custie platform serves two distinct participant types. Each is subject to a differentiated onboarding and verification process based on their role and associated risk profile.

2.1 Service Providers (KYB)

Service providers are pet-care professionals seeking to offer services through the platform. Two sub-classifications exist:

Provider Type	Description	Verification Requirements
Sole Proprietor	Independent contractors operating under their own name (e.g., dog walkers, pet sitters)	Government-issued photo ID. Business documents required only if formally registered under a separate entity.
Brick & Mortar Business	Established pet-care businesses with a physical location (e.g., grooming salons)	Government-issued photo ID + Business verification documents (registration, operating license, or equivalent)

All service provider applications also require submission of the following profile information:

- Purpose for joining the platform
- Services offered
- Years of experience in the pet-care industry
- General professional background information

2.2 Consumers (KYC)

Consumers are pet owners seeking to connect with service providers through the platform. Consumer verification is intentionally streamlined given the lower inherent risk profile of this participant type.

Consumer onboarding requires submission of:

- First and last name
- Email address
- Phone number
- Physical address
- Pet information (species, breed, relevant care details)
- Service preferences and stated reasons for joining the platform

Note: Physical photo identification is not required for consumers. Identity verification for this group focuses on profile completeness, data consistency, and stated intent.

3. Technology Stack & System Architecture

All onboarding infrastructure is custom-built by the Custie engineering team and hosted on Amazon Web Services (AWS). No third-party identity verification, fraud detection, or onboarding tools are utilized at this time.

Frontend	React, custom onboarding form and profile creation interface
Backend	Node.js, API endpoint receiving and processing form submissions
Database	MySQL (AWS RDS) storage of all participant data and application statuses
File Storage	Amazon S3, secure storage of uploaded identity and business documents

Alert System	Slack API, automated notifications to fraud operations upon new submission
Review Interface	Proprietary internal admin portal, AWS-hosted, restricted access

The fraud operations team has no direct access to GitHub or AWS infrastructure. All operational interaction occurs through the admin portal, which surfaces MySQL data and S3 document links in a structured review interface.

4. Onboarding & Verification Process

The end-to-end onboarding process follows a structured six-stage flow from application submission through account activation.

Stage 1: Application Submission

The applicant completes the onboarding form via the Custie platform frontend. All required fields are enforced at the form level; submission cannot be completed with missing mandatory information. This control eliminates the operational overhead of incomplete application review.

Upon submission, the backend API receives the data payload, validates it for integrity, and writes a new record to the MySQL database with a status of PENDING_REVIEW. Any uploaded documents are stored in Amazon S3, with the corresponding file path recorded in the database.

Stage 2: Notification & Queue Assignment

The submission event triggers an automated Slack API notification to the fraud operations channel, alerting the review team that a new application is awaiting action. The application enters the pending queue within the admin portal and remains in PENDING_REVIEW status until it is actioned.

Stage 3: Identity & Document Review

The fraud operations team logs into the proprietary admin portal and opens the pending application. The review encompasses:

For Service Providers:

- Cross-reference submitted name against government-issued photo ID
- Verify ID document authenticity such as assesses document quality, formatting, and consistency with known ID standards
- Confirm email address consistency with submitted identity information
- Review business verification documents where applicable
- Evaluate stated purpose, services offered, and professional background for legitimacy and platform fit

For Consumers:

- Verify profile completeness and internal data consistency

- Assess email, name, and address for anomalies or mismatches
- Review stated purpose and service preferences for alignment with platform intent

Stage 4: Risk Assessment & Decision

Following document and data review, the fraud operations team assesses the overall risk profile of the applicant. Key risk signals evaluated include:

- Identity mismatch: name on ID does not match submitted profile name
- Email anomaly: email address inconsistent with or unrelated to the applicant's identity
- Document quality issues: blurry, cropped, or altered ID uploads
- Stated intent: purpose or service description that raises integrity concerns or conflicts with platform values
- Profile inconsistency: information across fields that contradicts or conflicts internally

A decision is rendered: APPROVED or REJECTED. All decisions are recorded in the MySQL database, updating the application status accordingly.

Stage 5: Communication & Resolution

Approved applicants receive platform access notification through the application. Rejected applicants are notified via the platform with a description of the issue and instructions to correct or resubmit required information. Resubmitted applications re-enter the PENDING_REVIEW queue for a subsequent review cycle.

Stage 6: Account Activation

Upon approval, the backend updates the application status to ACTIVE, triggering account activation and granting the participant full platform access. For service providers, this enables profile visibility to consumers. For consumers, this enables service browsing and provider engagement.

5. Fraud Controls

Six fraud controls are embedded within the onboarding and platform integrity framework. All controls are operationalized without third-party tooling.

#	Control	Description
1	**KYC/KYB Identity Verification**	Government-issued ID required for all service providers. Business documents required for registered entities. Manual cross-referencing of submitted data against identity documents.
2	**Required Field Validation**	All mandatory fields enforced at the frontend form level. Applications cannot be submitted with incomplete information, preventing incomplete applications from entering the review queue.

3	**Data Minimization Control**	Onboarding data collection is limited to the minimum information necessary to make a sound approval decision. Reduces time-to-decision and minimizes unnecessary data exposure.
4	**Application Integrity Review**	Manual review of all submitted information for internal consistency, including name-to-email alignment, identity document verification, and stated purpose evaluation.
5	**Pre-Launch Threat Modeling**	Prior to platform launch, threat modeling is conducted across new account fraud and account takeover (ATO) vectors to identify and mitigate risk exposure before participant onboarding begins.
6	**Escalation & Review Workflow**	Structured review pipeline: submission → Slack alert → admin portal queue → manual review → approve/reject → MySQL status update. Defined escalation path for applications requiring additional scrutiny.

6. Decision Authority & Escalation

All onboarding decisions are made by the fraud operations manager, who serves as the sole decision authority for participant approvals and rejections. No automated decisioning tools are utilized at this time.

Escalation criteria warranting additional review or leadership involvement include:

- Applications with confirmed or suspected identity misrepresentation
- Business documents that cannot be verified through available means
- Applicants exhibiting behavioral patterns inconsistent with stated platform purpose
- Any application presenting novel risk signals not covered by existing review criteria

7. Operational Risk Metrics

The following metrics are tracked on an ongoing basis to monitor onboarding performance, decision accuracy, and platform integrity. Metrics are maintained in an internal operations tracker and used to iterate on controls and communicate risk posture.

True Positive Rate (TPR)	Measures the rate at which legitimate applicants are correctly approved
False Positive Rate (FPR)	Measures the rate at which legitimate applicants are incorrectly flagged or rejected
Approval Rate	Total approved applications as a percentage of total applications reviewed
Decline Rate	Total rejected applications as a percentage of total applications reviewed
Time-to-Decision (TTD)	Elapsed time from application submission to final approval or rejection decision
Fraud Incidents	Number of confirmed fraud events attributable to onboarded participants