CUSTIE PLATFORM

Pre-Launch Fraud Prevention Controls & Threat Modeling

Fraud Operations & Trust and Safety

Confidential | Internal Use Only

Document Owner	Fraud Operations & Trust and Safety
Classification	Confidential - Internal Use Only
Scope	Pre-launch fraud risk assessment and control design

1. Purpose

This document defines the fraud prevention controls and threat modeling executed prior to platform launch. Before any participant is onboarded, the fraud operations function conducts a structured threat modeling exercise to identify the most likely attack vectors the platform faces, assess their risk level, and ensure controls are in place to mitigate them before launch.

2. Threat Modeling Overview

Threat modeling is conducted across the two highest-priority attack vectors for a B2B/B2C platform of Custie's type: New Account Fraud (NAF) and Account Takeover (ATO). These vectors are prioritized based on the platform's structure, a two-sided marketplace connecting service providers with consumers and the inherent trust relationship required between participants.

The threat modeling process evaluates each vector across three dimensions: the specific attack scenario, the risk level to the platform and its participants, and the mitigation control designed to address it.

2.1 New Account Fraud (NAF)

New account fraud occurs when a bad actor creates a fraudulent account using false, stolen, or misrepresented identity information to access the platform for illegitimate purposes.

Threat Vector	Attack Scenario	Risk Level	Mitigation Control

False Identity Registration	Actor submits fabricated personal information and a counterfeit or stolen ID to gain platform access as a service provider	**High**	KYC/KYB identity verification with manual ID document review
Business Misrepresentation	Actor falsely claims to operate a legitimate pet-care business to gain provider status and consumer trust	**High**	KYB business document verification + stated purpose review
Benign Consumer, Harmful Intent	Actor registers as a consumer with accurate information but undisclosed intent to harm, exploit, or defraud a service provider	**Medium**	Stated intent review + post-onboarding behavioral monitoring
Duplicate Account Creation	Previously rejected or removed actor creates a new account under a different identity to regain platform access	**High**	Application integrity review + cross-reference against known rejected submissions
Incomplete or Manipulated Submission	Actor submits a partial or altered application to circumvent review requirements	**Medium**	Required field validation enforced at form level

2.2 Account Takeover (ATO)

Account takeover occurs when a bad actor gains unauthorized access to a legitimate participant's account, typically to exploit the trust and reputation that account has built on the platform.

Threat Vector	Attack Scenario	Risk Level	Mitigation Control
Credential Compromise	Actor obtains login credentials through phishing, reuse from other breaches, or social engineering to access a legitimate account	**High**	Escalation workflow + account suspension protocol on anomalous access signals
Provider Impersonation	Actor takes over a verified provider account to solicit consumers under a trusted identity	**High**	Post-onboarding behavioral monitoring + consumer complaint workflow
Consumer Account Exploitation	Actor takes over a consumer account to access provider contact information or manipulate service interactions	**Medium**	Behavioral monitoring + escalation framework
Profile Manipulation Post-Approval	Legitimate account holder or bad actor modifies verified profile information	**Medium**	Detection logic flag on post-approval profile

	after approval to misrepresent identity or services		changes inconsistent with verified ID

3. Pre-Launch Control Validation

Prior to launch, each fraud control is reviewed against the threat model to confirm it addresses risk vectors. The validation confirms that the six controls collectively cover all High and Medium risk scenarios identified during threat modeling.

Control	NAF Coverage	ATO Coverage
KYC/KYB Identity Verification	Prevents false identity and business misrepresentation at entry	Provides identity baseline for anomaly detection post-approval
Required Field Validation	Blocks incomplete or manipulated submissions	N/A, onboarding control
Data Minimization	Reduces attack surface by limiting data collected	Limits exposure of participant data in the event of a breach
Application Integrity Review	Detects fabricated or inconsistent identity information	Establishes verified identity baseline for comparison against future account activity
Pre-Launch Threat Modeling	Identifies and addresses all NAF vectors prior to launch	Identifies and addresses all ATO vectors prior to launch
Escalation & Review Workflow	Ensures NAF detections are escalated and actioned	Ensures ATO signals are escalated and actioned immediately

4. Proactive Risk Signal Monitoring

In addition to reactive controls, the fraud operations function establishes proactive monitoring practices prior to launching to maintain platform integrity. These practices are designed to surface risk signals before they escalate into incidents.

- Regular review of participant activity patterns for anomalies inconsistent with normal platform usage
- Monitoring of complaint volume and complaint patterns to identify emerging risk trends
- Cross-referencing new activity against known risk signals established during threat modeling
- Ongoing assessment of whether existing controls remain adequate as the participant base grows