Capital Investment Club

Transfer Processing Inventory

Public-safe inventory of confirmed and potential CIC transfer relationships, data categories, destinations, mechanisms, safeguards, and confirmation gaps.

Status: Draft for external legal and privacy review
Version: 0.9
Supersedes: None - initial publication
Last reviewed: 12 August 2026
Next review: 12 November 2026
Owner: Privacy and compliance owner - confirmation required
Approver: Executive owner and privacy counsel - pending

Document control	Value
Document ID	CIC-PIA-TIA-003
Version	0.9
Superseded version	None - initial publication
Status	Draft for external legal and privacy review
Publication classification	Public
Owner	Privacy and compliance owner - confirmation required
Approver	Executive owner and privacy counsel - pending
Effective date	Pending approval
Last reviewed	12 August 2026
Next review	12 November 2026 or earlier after a material change

Inventory rules

This public-safe inventory distinguishes evidence of an integration from evidence that an international transfer is active. It does not publish account identifiers, private endpoints, credentials, contract copies, precise security architecture, or personal data.

Risk scale: Low, Medium, Medium-High, High. No transfer is marked Approved until provider, destination, mechanism, safeguards, and owner approvals are confirmed.

Transfer register

ID	Transfer family and recipients	Data and subjects	Source to destination	Evidence state	Mechanism state	Residual risk
T-01	Google Cloud application hosting	All member, organization, transaction, KYC, support, audit, and technical data processed by the hosted services	Global users and CIC personnel to United States-hosted service; backup and support locations require confirmation	Hosting confirmed; exact product-region commitments require confirmation	Google contract, DPA, applicable SCC/UK terms, and Nigerian safeguard require owner evidence	Medium-High
T-02	Google Cloud object storage	Uploaded identity, support, recording, application, and public/private files depending bucket and workflow	Global/Nigeria/UK/EEA/Canada users to selected cloud bucket region; support locations require confirmation	Storage integration confirmed; active buckets and region controls require confirmation	DPA and transfer terms require owner evidence	High for Restricted files
T-03	MongoDB-compatible primary databases	Accounts, profiles, KYC, transactions, messages, support, audit, notification, and careers records	Global users to database region and provider support locations not confirmed	Database connectivity confirmed; provider and cluster location unconfirmed	Contract, DPA, transfer clauses, and subprocessor list not evidenced	High
T-04	Google OAuth and authentication services	Account identifier, email, profile, login, token, and security metadata	User jurisdiction to Google processing locations	Integration evidenced; production use requires confirmation	Provider terms and transfer scope require confirmation	Medium
T-05	CIC email and notification delivery providers	Email, name, preference, template content, security/workflow event, delivery and unsubscribe metadata	CIC services to selected email provider and subprocessors; exact provider/location unconfirmed	Notification delivery confirmed as a function; SendGrid, AWS SES, and Resend capabilities are evidenced	Active provider, DPA, location, and mechanism require confirmation	Medium-High
T-06	Paystack payment processing	Identity/contact, amount, currency, payment reference, status, and transaction metadata	User/CIC to Paystack processing and banking partners	Integration evidenced; production activation requires confirmation	Contract, DPA, onward recipients, and transfer basis require confirmation	High
T-07	Stripe payment and connected-account processing	Identity, business, payment, bank, transaction, webhook, and compliance data	User/CIC to Stripe and subprocessors, potentially United States and global locations	Integration evidenced; feature flags and production activation require confirmation	DPA, SCC/DPF scope, account country, and onward transfer require confirmation	High
T-08	Embedly wallet and bank-transfer services	Identity, wallet, account, bank-transfer, inflow, transaction, and webhook data	CIC and Nigerian users to provider processing locations	Integration evidenced; production use and provider entity require confirmation	Contract, DPA, location, and transfer basis require confirmation	High
T-09	Mono financial-data services	Identity, linked account, bank-data, transaction, and verification responses	CIC/user to provider and connected institutions	Integration evidenced; production use requires confirmation	Contract, DPA, connected-bank roles, retention, and transfer basis require confirmation	High

ID	Transfer family and recipients	Data and subjects	Source to destination	Evidence state	Mechanism state	Residual risk
T-10	Plaid financial-data services	Identity, account, balance, transaction, institution, token, and verification information depending enabled products	User/CIC to Plaid and connected institutions, potentially United States and supported regions	Integration evidenced; enabled products and countries require confirmation	Contract, DPA, transfer mechanism, and DPF status require confirmation	High
T-11	Google APIs and optional external media upload	Account authorization, media, metadata, and operational logs depending feature	CIC/user to Google service locations	Integration capability evidenced; production activation and media categories require confirmation	Provider terms and transfer scope require confirmation	Medium-High
T-12	Agora real-time video and cloud recording	User identity, channel/session, voice, video, screen content, recording metadata, and files	Global participants to Agora routing/recording and cloud storage locations	Integration and recording configuration evidenced; active routing and recording region require confirmation	Contract, DPA, consent, location, retention, and mechanism require confirmation	High
T-13	Electronic-signature provider	Names, emails, agreements, signatures, audit trail, and webhook metadata	CIC/user to selected provider location	Generic provider integration capability evidenced; provider identity unconfirmed	No provider-specific contract or transfer evidence reviewed	High until identified
T-14	GitHub source control and Actions	Source, configuration, workflow logs, test fixtures, issue evidence, and contributor information	CIC contributors and CI to GitHub processing locations	Use confirmed	Organization terms, DPA, evidence classification, and transfer treatment require owner confirmation	Medium
T-15	Public-site careers processing	Applicant identity/contact, resume, application, OAuth, security, and email metadata	Applicants globally to Google Cloud, database, object storage, OAuth, and email services	Workflow and integrations confirmed; active provider locations require confirmation	Same provider-specific mechanisms as T-01 to T-05	Medium-High
T-16	CIC personnel, contractors, reviewers, approvers, and support remote access	Data visible within each authorized role, potentially including Restricted identity and transaction records	Hosted systems to workforce access countries	Role controls evidenced; workforce country inventory not reviewed	Employment/contractor terms, confidentiality, access location, and transfer treatment require confirmation	High
T-17	External counsel, auditors, assessors, or incident responders	Selected governance, user, transaction, security, incident, or evidence records	CIC to recipient jurisdiction on a case-specific basis	Governance policies permit controlled sharing; no specific disclosure assessed	Case-specific necessity, confidentiality, mechanism, minimization, and record required	Medium-High to High

ID	Transfer family and recipients	Data and subjects	Source to destination	Evidence state	Mechanism state	Residual risk
T-18	Analytics, observability, error monitoring, and operational telemetry	Pseudonymous user or session reference, request, device, error, performance, security, and operational metadata; content must be excluded unless separately approved	CIC services to the selected telemetry provider and support locations, which are unconfirmed	Monitoring and analytics capability is evidenced; active providers and payloads require confirmation	Provider, location, DPA, transfer mechanism, retention, sampling, and redaction require confirmation	Medium-High

Transfer operating characteristics

ID	Exporter, importer, and role state	Frequency	Retention state	Accountable owner role	Review state
T-01	CIC controller/processor role and Google contracting entity require confirmation	Continuous while hosted workflows are used	CIC and provider schedule requires confirmation	Cloud infrastructure owner	Quarterly while Draft; pending approval
T-02	CIC and Google storage roles require confirmation per bucket and workflow	Event-driven uploads and retrieval	File-category and backup schedule requires confirmation	Cloud storage and records owners	Quarterly while Draft; pending approval
T-03	CIC role, database provider, and importer role are unconfirmed	Continuous application persistence	Collection-level, backup, and provider deletion schedule unconfirmed	Database infrastructure owner	Critical closure review; pending approval
T-04	CIC and Google identity roles depend on OAuth purpose and scope	At registration, sign-in, refresh, and revocation	Token, account, and security-log schedules require confirmation	Identity and access owner	Quarterly while Draft; pending approval
T-05	CIC role and active communications provider/importer require channel reconciliation	Event-driven notifications and campaigns	Message, delivery, suppression, and provider-log schedules require confirmation	Communications owner	Quarterly while Draft; pending approval
T-06	CIC, Paystack, and banking-partner roles require product confirmation	Per initiated payment and webhook	Financial, dispute, legal, and provider schedules require confirmation	Payments owner	Per active rail before approval
T-07	CIC, Stripe, connected-account, and banking roles require product confirmation	Per onboarding, payment, payout, and webhook	Financial, compliance, dispute, and provider schedules require confirmation	Payments owner	Per active product before approval
T-08	CIC, Embedly, and banking-partner roles require confirmation	Per wallet creation, transfer, inflow, and webhook	Wallet, transaction, legal, and provider schedules require confirmation	Wallet operations owner	Per active product before approval
T-09	CIC, Mono, and connected-institution roles require confirmation	Per consent, link, verification, refresh, and retrieval	Consent, token, bank-data, and provider schedules require confirmation	Banking-data owner	Per active product before approval

ID	Exporter, importer, and role state	Frequency	Retention state	Accountable owner role	Review state
T-10	CIC, Plaid, and connected-institution roles require confirmation	Per consent, link, verification, refresh, and retrieval	Product, token, bank-data, and provider schedules require confirmation	Banking-data owner	Per active product before approval
T-11	CIC and Google service roles depend on each enabled API	Event-driven by enabled feature	Authorization, media, metadata, and log schedules require confirmation	Product integration owner	Before each API activation
T-12	CIC and Agora roles depend on routing and recording configuration	During live sessions and recording jobs	Session, recording, backup, and deletion schedules require confirmation	Communications product owner	Critical if active; pending approval
T-13	CIC and electronic-signature provider roles are unconfirmed	Per agreement and webhook	Agreement, audit, legal, and provider schedules require confirmation	Legal operations owner	Provider identification required
T-14	CIC and GitHub roles depend on organization and Actions services	Continuous source collaboration and CI	Repository, issue, artifact, and log schedules require confirmation	Engineering operations owner	Annual and after material change
T-15	CIC controller role and cloud/database/email processor roles require confirmation	Per application and hiring workflow event	Applicant, attachment, communication, and legal schedules require confirmation	People operations owner	Quarterly while Draft; pending approval
T-16	CIC entity and personnel/contractor receiving roles require country and entity inventory	During authorized access sessions	Audit, support, and case schedules require confirmation	People and security owners	Critical closure review; pending approval
T-17	CIC and recipient roles are case specific	Exceptional or engagement based	Matter, audit, incident, legal-hold, and return/deletion terms apply	Legal and governance owners	Approval before each material disclosure
T-18	CIC and telemetry provider roles depend on selected service and payload	Continuous or sampled event delivery	Event, log, trace, error, and provider schedules require confirmation	Monitoring and security owners	Provider and payload review required

Required transfer details before approval

For every active row, the controlled provider register must record:

- CIC legal entity and exporter role.
- Provider legal entity and importer role.
- Product and account owner.
- Production activation state.
- Data fields and data-subject categories.
- Storage, processing, backup, support, and remote-access countries.
- Subprocessors and change-notification method.
- Contract, DPA, and security exhibit.

- Adequacy or certification scope where relied upon.
- SCC module, UK IDTA/Addendum, Nigerian safeguard, or other mechanism.
- Provider government-request policy and relevant request history where available.
- Encryption and key-control architecture.
- Retention, deletion, return, portability, and incident terms.
- Inherent and residual risk.
- Privacy, security, business, and legal approvals.

Data minimization rules by transfer

Transfer type	Minimum rule
Notifications	Do not place full financial identifiers, identity documents, credentials, or unnecessary case details in message templates or provider metadata.
Analytics	Use pseudonymous identifiers; exclude KYC documents, financial identifiers, message content, and precise location unless separately assessed.
Payments	Send only fields required by the selected rail and legal obligations; do not duplicate provider data into logs.
Recordings	Default recording off; require explicit consent where applicable; separate recording files from general public storage.
Support	Share the smallest record needed; use audited access and purpose-specific file requests.
Source and CI	Never use production personal data as fixtures; redact screenshots and logs before committing evidence.
Vendor support	Use time-limited access, masked evidence, and case-specific authorization where the provider supports it.

Onward transfers

Every active provider must have an approved subprocessor record. A provider's own public list is supporting evidence, not proof that CIC has subscribed to change notices, configured regional controls, or accepted current terms. CIC must evaluate material new subprocessors before the objection period expires where contractual rights exist.

Remote access

Remote access by a separate provider or workforce entity may constitute or contribute to an international transfer even when data remains stored in one region. CIC must inventory access countries for:

- Cloud and database support.
- Payment and verification provider support.
- CIC employees and contractors.
- Reviewers, approvers, support agents, and incident responders.

- Vendor engineers using customer-authorized troubleshooting access.

Approval status

All rows are Pending factual and legal confirmation unless a controlled evidence record records otherwise. Publication of this inventory does not activate, authorize, or approve an integration.

Related reports

- Transfer Impact Assessment (/governance/documents/transfer-impact-assessment)
- Transfer Vendor and Subprocessor Assessment (/governance/documents/transfer-vendor-and-subprocessor-assessment)
- Transfer Risk Register (/governance/documents/transfer-risk-register)

Limitation

This inventory was prepared with AI assistance from repository and governance evidence. Authorized owners must reconcile it against production consoles, contracts, invoices, vendor registers, and workforce records before approval.