

KAIRO FINANCE LIMITED

Description of Payment Services and Payment Processes

Attachment to the Bank of Canada RPAA Registration Application (Section 6.1)

Field	Detail
Applicant legal name	Kairo Finance Limited (trade name: “Kairo”)
Incorporation	Canada Business Corporations Act. Corporation No. 1809603-1, incorporated 16 July 2026
Registered office	1216-200 Old Carriage Dr, Kitchener, Ontario, N2P 0C7, Canada
Directors	Emmanuel Ayomide Abayomi (resident Canadian); Oluwatimilehin Abdulwahab Disu; Yusuf Ayomide Sodja
Related attachments	Payment flow diagrams; Consumer & Business Terms of Service; Safeguarding Framework; TPSP Register; Personal & Financial Information Inventory; Corporate Organisation Chart; RMIRF; AML Programme

1. Overview of the Applicant and its Services

Kairo Finance Limited (“Kairo”) is a Canadian federal corporation that will operate a multi-currency money-movement platform for individuals and businesses, with an initial focus on customers connected to the Nigeria–Canada corridor. Through the Kairo application, end users open an account, hold balances in supported fiat currencies, fund their account by bank transfer, transfer money to other Kairo users, send domestic and cross-border payments to third-party bank accounts, and pay merchants using payment cards issued under the Kairo programme.

Kairo has not begun operations and will not perform retail payment activities for end users in Canada prior to registration under the Retail Payment Activities Act (RPAA). The applicant serves end users in Canada; end users in other markets are served by affiliated entities. The Nigerian affiliate, KAIRO KONNECT LIMITED (RC 9622481), provides technology development, engineering and group operations to the applicant under an intercompany services agreement; it performs no retail payment activities on the applicant’s behalf. Konnect engineering personnel have production access to the applicant’s systems for deployment and operational support, with incidental access to Canadian customer data; that access is role-based, individually identified, MFA-protected, fully logged, reviewed quarterly under the applicant’s risk framework, and governed by data-processing terms in the intercompany services agreement. Canadian end-user data remains hosted in Canada and is not stored in Nigeria. A United Kingdom affiliate is planned within the next twelve months to serve UK end users and will be disclosed to the Bank upon incorporation.

Products

- Kairo (consumer): personal multi-currency account with balances, transfers, payouts, cross-border payments and cards.
- Kairo for Business: business accounts with team roles, sub-account balances (master, shared and individual), maker-checker approvals, batch (bulk) payments, spend controls and business cards, performing the same underlying payment functions.

2. Payment Functions Performed (RPAA Mapping)

RPAA payment function	Performed?	How Kairo performs it
Provision or maintenance of an account	Yes	Kairo provides ledger-based end-user accounts (not bank deposit accounts) holding fiat balances and the personal and financial information used for current and future EFTs; the ledger is operated by Kairo and hosted in Canada (AWS ca-central-1)
Holding of funds on behalf of an end user	Yes	End-user fiat balances are held until withdrawn, transferred or spent; funds are safeguarded as described in Section 6
Initiation of an EFT at the request of an end user	Yes	End users initiate transfers, payouts and card payments in the Kairo application; payments are customer-initiated and authenticated at initiation, with card-based recurring payments occurring under the cardholder’s standing authorization
Authorization of an EFT; transmission, reception or facilitation of instructions	Yes	Kairo authorises card transactions against end-user balances in real time, transmits payment instructions to its banking, payments and card partners, and receives card-network authorization requests and partner status callbacks
Clearing or settlement services	No	Kairo does not calculate or net final positions, transform or sort payment items for clearing or settlement, act as clearing/settlement agent for others, or post settlement entries for other participants

3. Payment Processes

The processes below correspond with the attached payment flow diagrams. All flows are performed in fiat currency only.

3.1 Account funding (collections)

The end user funds their Kairo account by sending a bank transfer from their external bank account to account details presented in the Kairo application. Inbound funds are received through Kairo's Canadian financial-institution partner, reconciled automatically to the end user, and credited to the end user's Kairo balance, with real-time notification. Funds are placed into the safeguarding account no later than the end of the business day following receipt.

3.2 Transfers between Kairo users

An end user initiates a transfer to another Kairo user in the application. Kairo authenticates the user, checks available balance and applicable limits, and records the movement between the two end users' balances on Kairo's ledger. Funds remain within the safeguarded pool; the transfer is reflected to both parties immediately.

3.3 Domestic payouts

An end user instructs a payment from their Kairo balance to a third-party bank account in Canada. Kairo authenticates the user and the instruction (with step-up authentication per limits), validates beneficiary details, debits the end-user balance, and transmits the payment instruction to its financial-institution/rails partner for execution over Canadian payment rails. Failed payouts are automatically reversed to the end-user balance.

3.4 Cross-border payments

An end user instructs a payment in one supported currency for delivery in another (for example, CAD to NGN). Kairo presents the full conversion rate and the exact amount the recipient will receive before the end user confirms. On confirmation, Kairo debits the end-user balance, performs the conversion at the quoted rate, and transmits the payout instruction to its destination-country payment partner for delivery to the recipient's bank account, with status updates until delivery.

3.5 Card transactions

End users may be issued virtual or physical payment cards linked to their Kairo balance. When the end user pays a merchant, the card network routes an authorisation request to Kairo's card programme; the transaction is authorised in real time against the end user's available balance and applicable card controls, and settled through the card network. Recurring and merchant-initiated card transactions occur under the cardholder's standing authorization for that card, subject at all times to available balance and the cardholder's controls (freeze, limits, merchant categories).

3.6 Business sub-accounts, approvals and batch payments

Business customers structure their money as a hierarchy of balances: one master balance per business with shared (team) and individual sub-balances, each holding pockets of supported currencies. Business roles gate access; transfers out of shared balances route through maker-checker approval. Businesses may also execute batch (bulk) payments: a payment group or uploaded file of up to [1,000] rows is validated (including beneficiary account-name verification where available), reviewed with totals per funding balance, approved under the business's approval rules, confirmed with step-up authentication, and executed row-by-row with per-row status, retry handling for failures, and full audit records. Each row is an EFT of the kinds described in 3.2–3.4.

4. Currencies

Kairo performs electronic funds transfers in the following fiat currencies: Canadian dollar (CAD), United States dollar (USD), pound sterling (GBP), euro (EUR) and Nigerian naira (NGN). For end users in Canada, held balances are offered in CAD, USD, GBP and EUR; NGN is supported as a conversion and payout currency only and is not held as a Canadian end-user balance. Kairo does not perform EFTs in digital currencies.

5. Activities Outside RPAA Scope

Kairo separately plans to offer a virtual-currency conversion service (the purchase and sale of fiat-backed stablecoins). That activity constitutes dealing in virtual currency under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. Kairo Finance Limited's FINTRAC status is currently In-View, pre-application submitted July 21, 2026, reference [78b12d17-a625-4b47-9ec5-06c1d02053d3]. The virtual-currency service will be conducted under that registration once effective, and will not be offered to persons in Canada before the registration is effective. Under current law, transfers of digital currency are excluded from the RPAA's definition of electronic funds transfer; the service is described here for completeness and transparency. Kairo monitors the development of the federal stablecoin framework and will update its registration should these activities come into RPAA scope.

6. Safeguarding of End-User Funds

- **FINAL METHOD:** end-user fiat funds will be held in trust in a dedicated, sole-purpose deposit trust account, segregated at all times from Kairo's own funds and used for no other purpose, constituting a valid express trust under Canadian law supported by a written legal opinion, per the Bank's Safeguarding End-User Funds Guideline.
- **Prospective safeguarding account provider:** Peoples Trust Company (Peoples Group), a federally regulated trust company (OSFI) and CDIC member. **NO AGREEMENT IS IN PLACE;** execution of the account agreement, declaration of trust and legal opinion are conditions precedent to launch. Alternate candidate: Digital Commerce Bank. Full detail: End-User Funds Safeguarding Framework (supporting document also attached).
- Funds received are placed into the safeguarding account as soon as practicable and no later than the end of the following business day; Kairo's ledger records each end user's entitlement individually and is reconciled daily against the safeguarding account; variances trigger immediate investigation and escalation under the RMIRF.

7. Key Third-Party Service Providers

Full records including addresses, materiality assessments, technology locations and data countries are in the TPSP Register v1.0. Providers marked prospective have no agreement in place.

Provider	Status	Service
Peoples Trust Company (Peoples Group)	PROSPECTIVE, no agreement	CAD accounts, safeguarding trust account, payment rails access; alternate: Digital Commerce Bank
VoPay International Inc.	PROSPECTIVE, under evaluation	EFT/Interac rails API connectivity
Sum and Substance Ltd (Sumsb)	PROSPECTIVE, under evaluation	Identity verification (KYC/KYB), screening and periodic re-screening
Amazon Web Services	PROSPECTIVE, standard terms	Cloud hosting, primary region Canada (Central) ca-central-1
Rain	PROSPECTIVE, under evaluation (USD programme)	Card issuing/processing infrastructure; Canadian card arrangements to be confirmed
BlockRadar	CONTRACTED	Digital-asset wallet infrastructure for the virtual-currency service (outside RPAA scope; no fiat-RPA dependency)

8. Compliance and Governance

- Risk management and incident response framework (v1.0): established per the RPAA and RPAR under Geraldine Oba, CAMLO & Oladipo Sadibo, COO, covering objectives and reliability targets, operational

risk and controls, incident response and business continuity including Bank notification, third-party risk, and annual review.

- AML programme (v1.1): customer identification, sanctions and PEP screening at onboarding and transaction time, risk-based periodic re-screening, transaction monitoring, record-keeping and reporting under the PCMLTFA, applied from onboarding.
- Payments are customer-initiated and authenticated at initiation; card-based recurring/merchant-initiated transactions occur under standing cardholder authorization subject to balance and controls; batch payments execute only after maker-checker approval and step-up confirmation. All activity is logged and auditable.
- Geographic controls: no retail payment activities for end users in Canada prior to RPAA registration; no virtual-currency services to persons in Canada prior to effective FINTRAC approval; residents of Quebec excluded at launch. Nigeria, a key destination corridor, was removed from the FATF list of jurisdictions under increased monitoring at the October 2025 FATF Plenary; Kairo's AML programme nonetheless applies a risk-based approach to all corridors, with enhanced due diligence and transaction monitoring calibrated to corridor risk.