AML Policy and Procedure

AuroSpace Payments Ltd.

Governing Framework: Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and FINTRAC Regulations

Revised: March 17, 2026

This policy was revised on March 17, 2026 to incorporate current FINTRAC regulatory requirements under the PCMLTFA, including amendments effective April 1, 2025 and October 1, 2025, and supersedes all prior versions.

AuroSpace Payments Ltd. (the Company) recognizes its obligations as a registered Money Services Business (MSB) in Canada and as a reporting entity under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), as administered and enforced by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). The Company is committed to the highest standards of Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Anti-Fraud compliance. The Board of Directors, Senior Management, and all employees are required to adhere to these standards and to ensure that the Company's services are not misused for money laundering, terrorist financing, sanctions evasion, or any other criminal purpose.

This policy is designed to reflect current FINTRAC regulatory requirements, including amendments to the PCMLTFA and associated Regulations that came into force on April 1, 2025 and October 1, 2025, and to align with the Financial Action Task Force (FATF) standards to which Canada is committed. This document constitutes the currently implemented AML/CTF compliance program of AuroSpace Payments Ltd.

1. Definitions

The following definitions apply throughout this policy and reflect terminology used in the PCMLTFA and FINTRAC guidance.

Know Your Customer (KYC) is the process by which the Company obtains information about the identity, address, and nature of business of its customers, ensuring that services are not misused by criminal elements for money laundering or terrorist financing.

Money Laundering refers to any direct or indirect attempt to indulge in, knowingly assist, or be a party to any process connected with the proceeds of crime and projecting such proceeds as untainted property, as defined under the PCMLTFA.

Proceeds of Crime means any property derived or obtained, directly or indirectly, as a result of criminal activity, or the value of any such property.

Customer means any person or entity that engages in a financial transaction or activity with the Company, including a person on whose behalf another person conducts a transaction, as defined under the PCMLTFA.

Transaction includes a purchase, sale, loan, pledge, gift, transfer, delivery, or arrangement thereof, and includes account openings, deposits, withdrawals, exchanges, or transfers of funds in any currency, whether by cash, cheque, payment order, electronic means, or other non-physical means.

Suspicious Transaction means any transaction or attempted transaction, whether or not completed and regardless of amount, that gives rise to reasonable grounds to suspect it may involve proceeds of a designated offence under the PCMLTFA, the financing of terrorist activities, unusual or unjustified complexity, or lack of economic rationale. FINTRAC requires all suspicious transactions to be reported regardless of the amount involved.

Politically Exposed Person (PEP) means an individual who is or has been entrusted with a prominent public function, including Heads of State or Government, senior politicians, senior government, judicial, or military officers, senior executives of state-owned corporations, or important political party officials, whether domestic or foreign. FINTRAC guidance updated in July 2025 extends PEP obligations to non-account-based reporting entity sectors, which applies to the Company.

Beneficial Owner (BO) means the natural person(s) who ultimately own or control a customer entity. For companies and partnerships, the threshold is ownership or control of more than 10% of shares, capital, or profits. For unincorporated associations, the threshold is 15%. For trusts, beneficial owners include the settlor, trustees, and beneficiaries with 10% or more interest. Where no natural person meets these thresholds, the senior managing official is treated as the

beneficial owner. For high-risk federal corporations incorporated under the Canada Business Corporations Act, the Company is required to consult the Corporations Canada database as part of beneficial ownership verification, effective October 1, 2025 per FINTRAC requirements.

Customer Due Diligence (CDD) means the process of identifying and verifying customers and their beneficial owners using reliable and independent sources, obtaining information on the purpose and nature of the business relationship, and taking reasonable steps to understand the customer's business, its ownership, and its control structure.

Large Cash Transaction means a cash transaction of CAD 10,000 or more, or multiple cash transactions totalling CAD 10,000 or more conducted by or on behalf of the same individual within a 24-hour window (the 24-hour aggregation rule). These must be reported to FINTRAC via a Large Cash Transaction Report (LCTR) within 15 calendar days of the transaction.

Electronic Funds Transfer (EFT) means any international electronic transfer of funds of CAD 10,000 or more initiated or finally received by the Company, including SWIFT and non-SWIFT transfers. The 24-hour aggregation rule applies, and such transfers must be reported to FINTRAC via an Electronic Funds Transfer Report (EFTR). Foreign currency amounts are converted to CAD using the Bank of Canada exchange rate at the time of the transaction.

Large Virtual Currency Transaction means the receipt of CAD 10,000 or more in virtual currency in a single transaction or in aggregated transactions from the same person within a 24-hour period. Pursuant to FINTRAC requirements in force since 2021 and reinforced under 2024-2025 directives, such transactions must be reported via a Large Virtual Currency Transaction Report (LVCTR) within 24 hours of receipt.

Compliance Officer / Principal Officer means the officer at management level designated by the Company as responsible for ensuring compliance with the PCMLTFA, all FINTRAC reporting and record-keeping obligations, and communication with FINTRAC on behalf of the Company.

2. Objectives

The objective of this AML/CTF policy is to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the financing of terrorist or criminal activities, in compliance with all applicable requirements under the PCMLTFA, its associated Regulations, and FINTRAC guidance. AuroSpace Payments Ltd. maintains adequate internal controls, documented procedures, and a risk-based compliance program that is reasonably designed and demonstrably effective. Under PCMLTFA amendments effective in 2025, a specific violation exists for programs that are not reasonably designed, risk-based, and effective, with administrative monetary penalties of up to CAD 20 million or 3% of gross global revenue for the most serious violations.

3. Regulatory Framework and FINTRAC Registration

AuroSpace Payments Ltd. operates as a registered Money Services Business under the PCMLTFA. Registration with FINTRAC is maintained as a prerequisite to operations and is kept current at all times. As a registered MSB, the Company is subject to the full suite of FINTRAC obligations covering client identification, record-keeping, transaction reporting, and compliance program requirements.

The Company's AML/CTF obligations are governed by the following legislative instruments and regulatory bodies:

- The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), S.C. 2000, c. 17, as amended through 2025
- The Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR), SOR/2002-184
- The Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations (PCMLTFSTRR), SOR/2001-317
- FINTRAC Guidance on Compliance Programs, Client Identification, Record Keeping, and Reporting, including MSB-specific record-keeping guidance updated September 2025
- The Retail Payment Activities Act (RPAA), administered by the Bank of Canada, to the extent applicable to the Company's payment activities
- The Personal Information Protection and Electronic Documents Act (PIPEDA), governing the handling of customer personal data

- FATF Recommendations, to which Canada's AML/CTF framework is aligned

The Company also complies with Ministerial Directives issued under the PCMLTFA, including current directives relating to Russia (updated March 2025), Iran (updated November 2025), and the Democratic People's Republic of Korea (updated March 2025). The Company monitors FINTRAC's official guidance portal at fintrac-canafe.canada.ca and implements required changes within applicable timeframes.

4. Applicability

This policy applies to all monetary transactions between AuroSpace Payments Ltd. and any counterparty, including customers, agents, correspondents, and business partners. The Board of Directors and Senior Management are responsible for ensuring adherence to this policy. All employees of the Company are bound by its provisions. Any third-party agent or mandatary acting on behalf of the Company in conducting transactions or verifying client identities remains subject to Company oversight and record-keeping obligations, and the Company retains full regulatory responsibility for their compliance under the PCMLTFA.

This policy will be reviewed at least annually and updated as required to reflect changes in FINTRAC guidance, PCMLTFA amendments, or changes in the Company's business activities. The effective date of this version is March 17, 2026.

5. Compliance Program Structure

The Company maintains a documented, comprehensive, and risk-based AML/CTF compliance program as required under the PCMLTFA. The compliance program consists of the five elements mandated by FINTRAC:

- Policies and procedures that establish how the Company meets its obligations under the PCMLTFA and associated Regulations
- A risk assessment that identifies and evaluates the ML/TF risks specific to the Company's business, products, delivery channels, customer types, and geographic reach
- Employee training covering AML/CTF obligations, the Company's compliance policies, and how to identify and report suspicious transactions and other reportable activities
- An ongoing compliance effectiveness review, conducted by a qualified person independent of the business lines being assessed, with findings reported to the Board at quarterly intervals
- A designated Compliance Officer responsible for day-to-day oversight of the compliance program and reporting to FINTRAC

Internal audit verifies compliance with KYC/AML policies and procedures, and consolidated notes on such audits are placed before the Audit Committee at quarterly intervals. Failure to adhere to this policy may result in disciplinary action, including termination of employment. Employees who suspect unethical behaviour are required to refer the matter to the Principal Officer.

6. Preventive Measures

The Company implements the following minimum preventive standards in line with FINTRAC requirements and the PCMLTFA.

Customer Acceptance Policy

Clear customer acceptance policies define which customers the Company will and will not accept, consistent with its risk appetite. The Company does not accept anonymous accounts or relationships where the beneficial owner cannot be identified. Customers in sectors on the Company's negative list or caution profiles are subject to enhanced scrutiny before acceptance.

Customer Identification Procedure

Identity verification is conducted at account opening or prior to completing a transaction of CAD 10,000 or more. For individuals, verification uses government-issued photo identification. For entities, the Company collects and verifies incorporation documents, governance documents, and the identity of directors and beneficial owners. At minimum, two standard KYC documents are collected per customer. Staff verify photocopies against originals and certify them with an 'Original Seen and Verified' stamp, their employee ID, and signature. A Unique Customer Identification Code (UCIC) is assigned to each customer to avoid multiple identities, track facilities, monitor transactions holistically, and support risk profiling.

Digital KYC

The Company implements digital KYC processes through its approved platform (Sumsub), capturing live photos of customers alongside officially valid documents, including the geographic location of the verification where applicable. Equivalent e-documents, meaning electronic equivalents issued by the originating authority with valid digital signatures, are accepted consistent with FINTRAC guidance.

Record Keeping and Retention

All transaction records and client identification records are maintained in accordance with FINTRAC's record-keeping requirements for MSBs, as updated in September 2025. Records must be retained for at least five years from the date of the transaction or the end of the business relationship, whichever is later, and must be producible to FINTRAC within 30 days of a request. Records include amounts and types of currency involved, the nature of the transaction, and all information sufficient to permit reconstruction of individual transactions for evidentiary purposes if required. KYC documents are preserved for at least five years after the business relationship ends. All documents are retained in a manner that permits reconstruction of individual transactions and are made available to competent authorities upon request.

Agent and Mandatary Oversight

Where the Company engages agents or mandataries to perform services on its behalf, the compliance program describes how those agents are supervised. Even where an agent performs identity verification, the Company retains full responsibility for all identification and record-keeping obligations under the PCMLTFA. Consistent with FINTRAC requirements effective October 1, 2025, the Company verifies that all agents and associated parties are not subject to Canadian sanctions and have not been convicted of money laundering, terrorist financing, or related offences. A registry of all agents is maintained, and initial verification of agents engaged prior to October 1, 2025 is completed no later than October 1, 2027.

Technology and IT Systems

The Company's IT systems are enabled to generate alerts when transactions are inconsistent with customer risk profiles. The Sumsub AML platform is used for customer risk screening and transaction monitoring, integrating sanctions, PEP, and adverse media data from multiple sources. The system supports automated suspicious activity detection and flagging, and generates reports for regulatory submission through FINTRAC's web reporting system (FWR). Virtual currency transaction monitoring is configured to identify Large Virtual Currency Transactions requiring LVCTR submission within 24 hours. AI-driven monitoring and continuous compliance review mechanisms are maintained to meet FINTRAC's expectation of proactive rather than reactive compliance.

New Products and Technologies

Prior to launching any new product, delivery mechanism, or technology, the Company conducts a risk assessment to identify ML/TF risks specific to that product or mechanism, consistent with FINTRAC guidance and FATF Recommendation 15. Appropriate risk mitigation measures are implemented before launch.

Employee Screening and Training

AML and KYC screening standards apply to all prospective employees at the time of recruitment. KYC documents for employees are maintained by Human Resources. Field staff are subject to household verification within 30 days of joining. Training programmes are maintained for all relevant roles and cover AML/CTF obligations, how to identify suspicious activity, reporting procedures, FINTRAC reporting thresholds, and the consequences of non-compliance. Training records are retained and updated as regulatory requirements evolve.

Fund Raising and Third-Party Relationships

Before entering into any arrangement for raising funds from any party other than a regulated bank or financial institution, Senior Management conducts sufficient due diligence on the counterparty. Any unusual or suspicious activity identified is reported to the Compliance Officer immediately.

7. Standard KYC Procedure

KYC verification is completed at account opening and updated periodically based on customer risk category. Customers are required to notify the Company of any changes to their submitted documents within 30 days of such changes. The update schedule is as follows:

- High risk customers: updated at least every two years
- Medium risk customers: updated at least every three years
- Low risk customers: updated at least every five years, or whenever a facility is renewed or replenished, whichever is earlier

KYC data is submitted to Credit Information Companies at the frequency and format stipulated by applicable Canadian regulation. Where the Company suspects money laundering or terrorist financing and reasonably believes that conducting CDD would tip off the customer, the CDD process is suspended and a Suspicious Transaction Report is filed with FINTRAC immediately.

8. Reliance on Third Parties for Customer Due Diligence

The Company may, at its option, rely on CDD conducted by a third party subject to the following conditions, consistent with FINTRAC guidance:

- Records or information from the third-party CDD are obtained immediately or from the Central KYC Records Registry
- The Company satisfies itself that copies of identification data and documentation can be obtained from the third party upon request without delay
- The third party is regulated, supervised, or monitored for compliance with CDD and record-keeping requirements
- The third party is not based in a jurisdiction assessed as high-risk
- Ultimate responsibility for CDD and enhanced due diligence remains with AuroSpace Payments Ltd. at all times

9. Risk Categorization of Customers

The Company categorizes all customers into low, medium, or high risk based on assessment and risk perception, including background, nature and location of activity, country of origin, sources of funds, and customer profile. Risk categorization is reviewed at Executive Committee level on a semi-annual basis to ensure timely identification of enhanced due diligence needs.

Low Risk

Individuals and entities whose identity and source of income can be easily verified, and whose transactions conform to a known profile. This category excludes customers in sectors on the Company's negative list or caution profiles.

Medium Risk

Individuals and entities listed under the negative list or caution profiles defined in the Company's Credit Policies or Operational Manual. Illustrative examples include jewelry traders and taxi operators.

High Risk

High net worth individuals, entities likely to pose above-average risk based on their background, nature of activity, country of origin, or sources of funds, and customers with complex or opaque ownership structures. PEPs of foreign origin are classified as high risk at a minimum and require the highest level of ongoing monitoring. For high-risk federal corporations incorporated under the Canada Business Corporations Act, the Company consults the Corporations Canada database to verify beneficial ownership, as required by FINTRAC from October 1, 2025.

10. Identification of Beneficial Owners

For any legal person or entity that is not a natural person, the Company identifies and verifies the beneficial owner(s) prior to or at account opening. In cases involving trust, nominee, or fiduciary accounts, the Company determines whether the customer is acting on behalf of another person and obtains satisfactory evidence of identity of all intermediaries and the persons on whose behalf they act. The nature of the trust or arrangement is documented. Beneficial ownership records are updated as part of ongoing CDD and following any changes to the customer's ownership or control structure. For high-risk federal corporations, the Corporations Canada database is consulted both at onboarding and during ongoing monitoring, as mandated by FINTRAC.

11. Transaction Monitoring

The Company conducts ongoing monitoring of customer transactions using the Sumsub platform, which integrates KYC data with transaction activity to produce a complete picture of customer behaviour. The system is configured to flag and escalate transactions that:

- Involve large or complex amounts with no apparent economic rationale or legitimate purpose
- Exceed thresholds prescribed for specific account categories or customer risk profiles
- Involve large amounts of cash inconsistent with the normal and expected activity of the customer
- Are linked to virtual assets, high-risk jurisdictions, or sanctioned parties
- Appear to be structured to avoid reporting thresholds

All unusual operations in any account are reported immediately to the Compliance Officer. Transaction monitoring rules and scenarios are reviewed and updated regularly to reflect evolving ML/TF typologies and FINTRAC indicators published for MSBs.

12. Reporting Requirements

As a reporting entity under the PCMLTFA, AuroSpace Payments Ltd. is required to submit the following reports to FINTRAC through the FINTRAC Web Reporting System (FWR):

Suspicious Transaction Reports (STR)

An STR must be submitted as soon as practicable after the Company completes measures that lead to reasonable grounds to suspect a transaction or attempted transaction is related to money laundering or terrorist financing. There is no monetary threshold for STR reporting. The Principal Officer records the reasons for treating any transaction as suspicious. Branch Heads and Area Managers are responsible for escalating suspicious activity to the Principal Officer promptly. STRs cover both cash and non-cash transactions, including attempted transactions.

Large Cash Transaction Reports (LCTR)

An LCTR must be submitted to FINTRAC within 15 calendar days when the Company receives cash of CAD 10,000 or more from a single person or entity, or when multiple cash amounts received from the same person or entity within a 24-hour window aggregate to CAD 10,000 or more.

Electronic Funds Transfer Reports (EFTR)

An EFTR must be submitted for any international electronic funds transfer of CAD 10,000 or more that the Company initiates or finally receives, including SWIFT and non-SWIFT transfers. The 24-hour aggregation rule applies. Foreign currency amounts are converted to CAD using the Bank of Canada exchange rate at the time of the transaction.

Large Virtual Currency Transaction Reports (LVCTR)

An LVCTR must be submitted within 24 hours when the Company receives virtual currency of CAD 10,000 or more from the same person within a 24-hour period. This obligation has applied since 2021 and is reinforced under current FINTRAC directives, which also extend to transactions linked to high-risk jurisdictions.

Listed Property and Terrorist Property Reports

The Company must report immediately to FINTRAC, the RCMP, and CSIS any property in its possession or control that is owned or controlled by a listed terrorist entity under the Criminal Code or the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism. The Company also integrates Listed Property Event and Property Report (LPEPR) procedures into the compliance program and retains reports in line with FINTRAC's five-year record-keeping requirements.

Ministerial Directive Compliance

The Company complies with all Ministerial Directives issued under the PCMLTFA, including current directives relating to Russia, Iran, and the DPRK. Transactions subject to Ministerial Directives are subject to enhanced scrutiny and, where applicable, are reported to FINTRAC in the format and within the timelines specified in the relevant directive.

13. Combating the Financing of Terrorism

The Company ensures that it does not maintain any account in the name of individuals or entities appearing on lists of individuals and entities suspected of having terrorist links, as approved and periodically circulated by the United Nations Security Council (UNSC). The relevant lists include:

- The ISIL (Da'esh) and Al-Qaida Sanctions List, maintained pursuant to Security Council resolutions 1267/1989/2253, available at scsanctions.un.org
- The Taliban Sanctions List, maintained pursuant to Security Council resolution 1988 (2011)
- All other UNSCRs circulated in respect of any other jurisdictions or entities from time to time

These lists are screened on a daily basis using the Trackwiz automated tool. Any modifications to the lists in terms of additions, deletions, or other changes are taken into account by the Company for meticulous compliance. Where a match is identified, the Company does not carry out the transaction, freezes any relevant funds or assets held, and immediately informs the relevant regulatory authority of the transaction details, including full particulars of the funds, financial assets, or economic resources involved. The Company also complies with Canadian sanctions obligations under the Special Economic Measures Act and the Justice for Victims of Corrupt Foreign Officials Act, and monitors applicable sanctions designations, including those covered by Ministerial Directives.

14. Preservation of Records

The Company maintains transaction records for at least five years from the date of the transaction, consistent with FINTRAC's record-keeping requirements for MSBs as updated in September 2025. All necessary records of both domestic and international transactions, including amounts and types of currency involved, are retained to permit reconstruction of individual transactions for evidentiary purposes if required. Records pertaining to customer identification and address, including copies of passports, identity cards, driving licences, and utility bills obtained at account opening and during the business relationship, are retained for at least five years after the business relationship ends. All records are maintained in a manner that allows them to be provided to FINTRAC within 30 days of a request.

15. Risk Assessment

The Company maintains a documented risk assessment that identifies and evaluates the ML/TF risks arising from its business activities, including its products and services, delivery channels, customer types, and geographic reach. The risk assessment is reviewed and updated at least annually, or when a material change occurs in the Company's business, and is made available to FINTRAC upon examination. The risk assessment informs the design and calibration of all preventive controls, monitoring thresholds, and CDD procedures described in this policy.

16. Internal Control System

All employees of AuroSpace Payments Ltd. conduct themselves in accordance with the highest ethical standards and carry out business in accordance with this policy. The following measures are maintained to implement AML/CTF requirements effectively:

- A risk-based approach to the management and mitigation of ML/TF risks, aligned with FINTRAC's risk-based compliance framework
- Clear allocation of responsibility for implementation of policies and procedures across all business lines
- Independent evaluation by the compliance function of policies, procedures, and legal and regulatory requirements
- Concurrent and internal audit to verify compliance with KYC/AML policies and procedures
- Consolidated reporting on audits and compliance to the Audit Committee at quarterly intervals
- A compliance effectiveness review conducted by a qualified, independent person, the results of which are used to improve the compliance program on a continuous basis

17. Principal Officer and Designated Director

In AuroSpace Payments Ltd., the Managing Director serves as the Designated Director for purposes of the PCMLTFA. The Principal Officer is the Company Secretary and Chief Compliance Officer, designated by the Company as responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law and FINTRAC regulations.

The Principal Officer ensures that adequate measures are taken to update the provisions of all policies framed in line with this policy, acts as custodian of this policy, shares periodic AML reports with the Executive Committee and Board, submits unusual and suspicious activity to regulatory and law enforcement authorities, and builds adequate awareness of AML/CTF requirements across the organization. The Principal Officer also serves as the primary point of contact with FINTRAC and is responsible for the timely submission of all required reports through the FINTRAC Web Reporting System.

18. Customer Screening and Transaction Monitoring

The Company uses Sumsub as its primary AML software for customer risk screening and transaction monitoring. Sumsub's database integrates sanctions, PEP, and adverse media data from multiple global sources, enabling comprehensive risk control at the point of customer onboarding and on an ongoing basis. Screening covers the full range of FINTRAC-required checks: sanctions screening, PEP identification, adverse media review, and ongoing transaction pattern analysis.

Transaction monitoring within Sumsub uses information from KYC processes to assign customer risk scores, which are then applied as part of rule-based scenarios to identify account-based activities warranting investigation or FINTRAC disclosure. Where the Company suspects money laundering or terrorist financing and reasonably believes that performing CDD would tip off the customer, the CDD process is not pursued, and an STR is filed immediately.

19. Conclusion

This policy sets out the AML/CTF compliance framework of AuroSpace Payments Ltd. as a registered MSB under the PCMLTFA and as a reporting entity subject to the full scope of FINTRAC's regulatory requirements. It specifies preventive measures, KYC and CDD procedures, transaction monitoring and reporting obligations, record-keeping standards, and the responsibilities of the Principal Officer and all employees. The policy is reviewed at minimum annually and updated to reflect evolving FINTRAC guidance, PCMLTFA amendments, and changes in the Company's business activities. All employees are expected to be familiar with its contents and to report any concerns about potential non-compliance to the Principal Officer promptly.

Annexure 1: Officially Valid Documents

The following documents are accepted for KYC purposes across AuroSpace Payments Ltd. business segments, consistent with FINTRAC's client identification requirements:

Individual Accounts

- Passport
- Government-issued Identity Card
- Driving Licence

Corporate Accounts

- Certificate of incorporation
- Memorandum and Articles of Association
- Board resolution and power of attorney granted to officers or employees authorized to transact
- Officially valid document in respect of managers or officers holding a transacting authority
- Names of persons holding senior management positions
- Registered office and principal place of business, if different

Partnership Accounts

- Registration certificate
- Partnership deed
- Officially valid document of the person holding a transacting authority
- Names of all partners
- Address of registered office and principal place of business, if different

Trust Accounts

- Registration certificate
- Trust deed
- Officially valid document of the person holding a power of attorney to transact
- Names of beneficiaries, trustees, settlor, and authors of the trust
- Address of the registered office of the trust

- List of trustees and supporting identity documents for those authorized to transact on behalf of the trust