MONESTO FINANCE

PRIVACY POLICY

Personal Information Protection, Data Governance and Privacy Breach Response Framework

Canada | Version 1.0 | 2026

Prepared for MONESTO FINANCE, a registered business name of CITADEX FINANCE INC.

Business Identification Number (BIN): 1001604553

Principal place of business	300 Supertest Road, Unit 1, North York, Ontario, M3J 2M2, Canada
Business activity	Financial transactions processing, reserve and clearing house activities (NAICS 52232)
Core privacy law	Personal Information Protection and Electronic Documents Act (PIPEDA)
Operational regulatory context	PCMLTFA and Regulations, FINTRAC guidance for MSBs, Canadian sanctions laws, travel rule obligations and applicable record-keeping requirements

Document Information

Document title	Privacy Policy
Entity / business name	MONESTO FINANCE
Registrant / legal holder	CITADEX FINANCE INC. (as reflected in Ontario business name registration)
Business Identification Number (BIN)	1001604553
Issue date	01.07.2026

Document Revision History

Version	Date	Author / Owner	Description of change
1.0	01.07.2026	Board of Directors / Privacy Officer	First issued version adapted for MONESTO FINANCE

Contents

1. Basic Provisions

MONESTO FINANCE is a registered business name used by CITADEX FINANCE INC. in Ontario, Canada. The business name registration identifies MONESTO FINANCE under Business Identification Number (BIN) 1001604553, with its principal place of business at 300 Supertest Road, Unit 1, North York, Ontario, M3J 2M2, Canada.

MONESTO FINANCE conducts, or intends to conduct, financial transactions processing, reserve and clearing house activities. In this context, the business may collect, use, disclose, retain and protect personal information relating to clients, prospective clients, beneficial owners, directors, officers, authorized users, counterparties, employees, consultants, suppliers and other individuals with whom it interacts.

This Privacy Policy sets out the principles, governance arrangements and operational standards by which MONESTO FINANCE handles personal information in accordance with the Personal Information Protection and Electronic Documents Act (PIPEDA), applicable Canadian privacy requirements and the business obligations arising from its financial services, anti-money laundering, anti-terrorist financing, sanctions and payment-related compliance framework.

2. Scope and Applicability

This Policy applies to all personal information under the custody or control of MONESTO FINANCE, whether collected directly from an individual, from a corporate client, from an authorized representative, from a public or commercial source, from a compliance screening provider, from a payment counterparty, from an affiliate or service provider, or from another lawful source.

- Clients and prospective clients, including individuals acting on behalf of corporate clients;
- Directors, officers, beneficial owners, authorized signatories and representatives of clients;
- Employees, contractors, consultants and applicants, to the extent applicable;
- Service providers, vendors, banking partners, payment counterparties and compliance-screening providers;
- Any person whose personal information is processed as part of onboarding, due diligence, transaction monitoring, reporting, complaints handling, privacy requests, legal obligations or business administration.

Where MONESTO FINANCE processes personal information on behalf of another organization, it will do so in accordance with the applicable contract, confidentiality obligations, privacy requirements and regulatory obligations.

3. Privacy Principles

MONESTO FINANCE follows the core privacy principles reflected under PIPEDA and Canadian privacy guidance. These principles are embedded in the Company's operating procedures, staff responsibilities, vendor oversight arrangements and record-keeping practices.

Accountability	MONESTO FINANCE is responsible for personal information under its control and designates a Privacy Officer to oversee compliance.
Identifying purposes	The purposes for collection, use and disclosure are identified at or before the time information is collected, unless permitted or required by law.
Consent	Consent is obtained where required, subject to legal exceptions, contractual necessity and regulatory obligations.
Limiting collection	Only information that is reasonably necessary for

	identified business, legal, regulatory or compliance purposes is collected.
Limiting use, disclosure and retention	Personal information is used, disclosed and retained only for identified purposes, as otherwise consented to, or as permitted or required by law.
Accuracy	Reasonable steps are taken to ensure personal information used for decisions is accurate, complete and up to date.
Safeguards	Administrative, physical and technical safeguards are applied based on the sensitivity of information.
Openness	The Company makes information about its privacy practices available to individuals.
Individual access	Individuals may request access to their personal information, subject to verification and legal limitations.
Challenging compliance	Individuals may raise privacy questions or complaints with the Privacy Officer.
Breach response	Privacy incidents are assessed, contained, investigated, documented and, where required, reported and notified.

4. Information We Collect

The personal information collected by MONESTO FINANCE will depend on the relevant relationship, product, service, transaction, regulatory obligation or operational context. Information may include:

- Identity information, such as name, date of birth, nationality, identification document details and verification information;
- Contact information, such as residential address, business address, email address and telephone number;
- Corporate and role information, including directorship, ownership, beneficial ownership, authorized signatory status and power of attorney information;
- Financial and transaction information, including source of funds, source of wealth, payment instructions, transaction history, account references, counterparty information and supporting documents;
- Compliance information, including customer risk profile, due diligence and enhanced due diligence records, sanctions and politically exposed person screening results, adverse media review outcomes and transaction monitoring alerts;
- Device, access and technical information, where services are delivered through digital platforms, portals, websites or secure communication channels;
- Communications and complaints information, including emails, letters, call notes, service requests, privacy requests and complaint records;
- Employment, contractor and vendor information, where relevant to administration, security, compliance and governance.
-

MONESTO FINANCE does not knowingly collect more personal information than is reasonably necessary for the relevant purpose. Where information is collected for compliance with PCMLTFA, FINTRAC guidance, sanctions legislation, the travel rule or other legal obligations, failure to provide required information may prevent MONESTO FINANCE from onboarding a client, processing a transaction or maintaining a business relationship.

5. Purposes for Collection, Use and Disclosure

MONESTO FINANCE collects, uses and discloses personal information for legitimate business, operational, legal and regulatory purposes, including:

- Establishing, managing and administering client relationships;
- Conducting know-your-client, identity verification, beneficial ownership verification, sanctions screening, politically exposed person screening and other AML/ATF controls;
- Processing, monitoring, reconciling and investigating financial transactions;
- Applying the travel rule for electronic funds transfers and virtual currency transfers, where applicable;
- Detecting, preventing and investigating fraud, unauthorized activity, money laundering, terrorist financing, sanctions evasion, cyber incidents and other unlawful or suspicious activity;
- Meeting obligations under the PCMLTFA and Regulations, FINTRAC guidance for MSBs, the Criminal Code provisions relating to terrorist property, the Special Economic Measures Act, the Justice for Victims of Corrupt Foreign Officials Act, the United Nations Act and related regulations;
- Responding to requests from regulators, law enforcement, courts, administrative tribunals, government authorities, auditors, banks, payment partners and other competent parties, where permitted or required by law;
- Managing complaints, disputes, privacy requests, legal claims and internal investigations;
- Operating, securing, testing and improving systems, controls, platforms, websites and communication tools;
- Maintaining records, audit trails and management information for governance, compliance, financial accounting, tax, reporting and oversight purposes.

6. Consent and Legal Exceptions

MONESTO FINANCE will obtain consent for the collection, use and disclosure of personal information where required. Consent may be express or implied, depending on the sensitivity of the information, the nature of the relationship and the reasonable expectations of the individual. Consent may be obtained through application forms, agreements, onboarding documentation, portal notices, website notices, written communications or other appropriate methods.

Individuals may withdraw consent at any time, subject to legal, contractual, regulatory and business limitations. A withdrawal of consent may affect MONESTO FINANCE's ability to provide services, process transactions, maintain a client relationship or comply with applicable law.

MONESTO FINANCE may collect, use, disclose or retain personal information without consent where permitted or required by law, including for AML/ATF reporting, sanctions compliance, fraud prevention, legal proceedings, regulatory examinations, suspicious transaction reporting, court orders, audits, investigations or other compliance purposes.

7. Disclosure and Transfers

MONESTO FINANCE does not sell client personal information. Personal information may be disclosed only where authorized, necessary, permitted or required. Disclosures may be made to:

- Affiliates, officers, employees, contractors and internal functions on a need-to-know basis;
- Banks, payment service providers, financial institutions, correspondent partners, clearing partners and transaction counterparties to process or investigate transactions;
- Technology, cloud, cybersecurity, data hosting, identity verification, screening, analytics, record-management and professional service providers;
- Regulators, FINTRAC, law enforcement authorities, courts, administrative tribunals and government bodies, where permitted or required;
- Auditors, legal counsel, consultants, insurers and other professional advisers;
- A successor, assignee, purchaser or prospective purchaser in connection with a reorganization, merger, sale, transfer or business continuity event, subject to appropriate safeguards.

Where personal information is transferred to a service provider or processed outside Canada, MONESTO FINANCE will use contractual, organizational and technical safeguards appropriate to the sensitivity of the information. Individuals should be aware that information processed outside Canada may be subject to lawful access by foreign courts, regulators or government authorities in accordance with local laws.

8. Safeguards and Access Controls

MONESTO FINANCE protects personal information using safeguards appropriate to the sensitivity, volume, format, location and risk profile of the information. Safeguards may include:

- Role-based access controls, least-privilege access, segregation of duties and approval controls;
- Secure onboarding and offboarding of employees, contractors and system users;
- Confidentiality obligations for staff, contractors and service providers;
- Password controls, multi-factor authentication where appropriate, secure storage and encryption where feasible;
- Secure transmission methods for sensitive documents and payment-related information;
- Physical controls over offices, filing cabinets, paper records and visitor access;
- Logging, monitoring, audit trails and periodic review of access rights;
- Staff training on confidentiality, privacy, information security, phishing, breach reporting and regulatory confidentiality obligations;
- Vendor due diligence and contractual controls for service providers handling personal information.

Employees and contractors must not access, download, copy, share or use personal information unless required for their role and approved business purpose. Any suspected unauthorized access, loss, theft, misuse or disclosure must be escalated immediately to the Privacy Officer and senior management.

9. Retention and Disposal

MONESTO FINANCE retains personal information only for as long as reasonably necessary to fulfil the purposes for which it was collected, to provide services, to administer relationships, to comply with legal and regulatory requirements, to maintain audit trails, to defend legal claims, or to meet applicable accounting, tax, AML/ATF, sanctions, FINTRAC and record-keeping obligations.

Retention periods may differ depending on the type of record and applicable legal requirement. Where AML/ATF, transaction monitoring, suspicious activity, sanctions, travel rule or regulatory reporting records must be retained, MONESTO FINANCE will retain those records in accordance with applicable laws and internal records retention schedules.

When information is no longer required, it will be securely deleted, destroyed, anonymized or archived in accordance with the Company's records retention and disposal procedures. Disposal methods must be appropriate to the sensitivity and format of the information.

10. Individual Access, Correction and Withdrawal of Consent

Individuals may request access to personal information held by MONESTO FINANCE, request correction of inaccurate or incomplete information, or withdraw consent where consent remains the lawful basis for processing. Requests must be made in writing to the Privacy Officer and must include sufficient information to allow MONESTO FINANCE to verify identity and locate the relevant records.

- MONESTO FINANCE may require government-issued identification or other verification measures before disclosing personal information;
- Requests will be handled within a reasonable time and in accordance with applicable law;
- Access may be refused or limited where permitted by law, including where disclosure would reveal confidential commercial information, information about another person, privileged information, information relating to an investigation, AML/ATF reporting information, sanctions controls, suspicious transaction analysis or information that MONESTO FINANCE is legally restricted from disclosing;
- Where a correction is justified, MONESTO FINANCE will update its records or note the request and its decision in the relevant file.

11. Privacy Breach Management

A privacy breach means the loss of, unauthorized access to, or unauthorized disclosure of personal information resulting from a breach of the Company's security safeguards or failure to establish appropriate safeguards. Examples include misdirected emails, lost devices, unauthorized system access, ransomware, accidental disclosure, theft of paper files, credential compromise or inappropriate internal access.

MONESTO FINANCE will maintain a structured privacy breach response process consisting of:

- Immediate containment and mitigation of the incident;
- Internal escalation to the Privacy Officer, senior management, information security and legal counsel, where required;
- Assessment of the nature, scope and sensitivity of the information involved;
- Assessment of whether the breach creates a real risk of significant harm to affected individuals;
- Notification to affected individuals and reporting to the Office of the Privacy Commissioner of Canada where required by PIPEDA;
- Notification to other organizations, regulators, financial institutions, law enforcement or service providers where appropriate to reduce or mitigate harm;
- Root cause analysis, remedial actions, control enhancements and staff retraining where necessary;
- Maintenance of breach records, whether or not the breach is reportable.

Significant harm may include bodily harm, humiliation, damage to reputation or relationships, loss of employment or business opportunities, financial loss, identity theft, negative effects on credit records or damage to or loss of property. Breach records must contain sufficient information to allow the Company to demonstrate that it assessed the incident appropriately and complied with reporting and notification obligations.

12. Complaints and Contact Details

Individuals may contact MONESTO FINANCE with questions, access requests, correction requests, consent withdrawal requests or complaints relating to the handling of their personal information.

Privacy Officer	Waqas Ali
Email	waqas.ali@monesto.io
Postal address	300 Supertest Road, Unit 1, North York, Ontario, M3J 2M2, Canada
Telephone	+14378879558
Complaint escalation	If unresolved internally, an individual may contact the Office of the Privacy Commissioner of Canada or another competent privacy authority, as applicable.

MONESTO FINANCE will investigate privacy complaints fairly, objectively and within a reasonable timeframe. Individuals will be informed of the outcome of the review and any corrective action that may be taken, subject to confidentiality, legal privilege and regulatory limitations.

13. Training, Monitoring and Review

The Privacy Officer, with support from senior management and relevant control functions, is responsible for maintaining this Policy, monitoring compliance, supporting staff awareness and ensuring that privacy risks are considered when the business introduces new systems, vendors, products, processes or geographies.

- This Policy will be reviewed at least annually and whenever there is a material change to legal requirements, business activities, technology, vendors, services or risk exposure;
- Employees and contractors with access to personal information will receive privacy and confidentiality training appropriate to their role;
- The Company will periodically review access rights, breach logs, privacy requests, vendor arrangements and data retention practices;

- Material privacy issues will be escalated to senior management and, where appropriate, to the Board or designated governance forum.

14. Annex A - Privacy Request Form

Individuals may use the following form to request access to personal information, request a correction, withdraw consent or raise a privacy complaint.

Full name	
Relationship to MONESTO FINANCE	Client / prospective client / representative / employee / other
Contact details	
Type of request	Access / correction / consent withdrawal / complaint / other
Description of request	
Relevant dates, accounts or transactions	
Supporting documents attached	Yes / No
Preferred response method	Email / postal mail / other
Signature and date	