BRINKS ETHICS & COMPLIANCE

# BRINK'S CANADA LIMITED ANTI-MONEY LAUNDERING POLICY

JULY 2024

# TABLE OF CONTENTS

# ABOUT BRINK'S CANADA LIMITED

Brink's Canada Limited ("Brink's" or the "Company), a publicly traded company, has been operational for 96 years and has a total of 39 branches within Canada. The Company has a registered office in Etobicoke, Ontario. Typically, Brink's Canada focuses its operations within Canada. If a client requires international transportation services with Canada being either the sending or receiving country, the Company relies on Brink's Global Services International, Inc., or Brink's Global Services entity in the respective country (collectively, "BGS") to complete the transport. BGS operates globally in 52 countries worldwide (see the Company's Anti-Money Laundering/Counter-Terrorism Financing (AML/CTF) Risk-Based Approach Methodology {the "Risk Assessment"}). However, such international transports constitute less than one percent of Brink's Canada's overall business.

The Company offers its services to entity customers as well as individual customers (collectively referred to as "customers"). Occasionally, Brink's offers valuable transport services to individual customers through BGS to transport precious metals. Additionally, on a rare occasion, Brink's may provide transportation of foreign currency under its low volume parcel ("LVP") services to individual customers. These are the only services available to individual customers, while all other products and services offered by Brink's are exclusively for entity customers.

The Company offers secure transportation services of cash, money orders, traveller's cheques, and other negotiable instruments. Brink's also transports precious metals like gold, silver, and occasionally palladium, along with other valuable assets, including stocks, bonds, and fine artwork. Brink's offers precious metals storage, cash processing, treasury management, ATM service, and cash vault services. Additionally, Brink's offers "Specials," which are one-off pick-ups. This service is often requested by longstanding customers who contact Brink's customer service or sales team, and a contract is established between the customer and Brink's before the service is provided.

Some of the services provided by the Company are considered covered activities under the PCMLTFA, and some activities are not in scope. The following table describes each service and whether they are in or out of scope:

| Service | In Scope/Out of Scope | Description of Service |
|---|---|---|
| Cash in Transit ("CIT") | In Scope | Brink's offers CIT services, which involves securely transporting cash to customer locations.<br>The Company primarily transports cash from a customer's business location to a financial institution or vice-versa.<br>Additionally, the Company may transport cash between two business locations of the same entity customer (for example: cash is transported between location A and location B of a single entity customer) and not residential locations.<br>The Company may pick up and transport cash in Canadian Dollar ("CAD"), the United States Dollar ("USD"), and other international currencies when requested by customers. In some cases, the Company picks up funds from contracting entities' agents.<br>The Company primarily transports cash within Canada or to the United States ("U.S.") only. |

| | | |
|---|---|---|
| | | Additionally, under its CIT services, the Company may also transport physical cheques to the customer's requested destination. Brink's does not process and/or cash these cheques.<br>Under this service, cash does not go through the processing centre before it is delivered to the customer's location. |
| Fiat ATM<br>• Pick-up<br>• Replenishment<br>• Holding in treasury | In Scope | Brink's offers ATM services, which includes cash replenishment and treasury management.<br>Brink's armoured trucks collect cash from various fiat ATM locations and transport it to a processing centre (either Brink's or a third-party) and go into treasury on behalf of the customer. Treasury services can be provided by Brink's or another third-party.<br>Once the cash is processed and validated through the processing centre (Brink's or third party), it is prepared for redistribution and delivered directly to the customer's business location.<br>Brink's may also collect cash from fiat ATMs and deliver it directly to the customer's business location. Funds are never delivered to a residential location.<br>The funds are never removed from an ATM and directly delivered to another ATM location until the cash has been through the processing centre, placed into treasury, and then prepared to be transported to another ATM.<br>Brink's processes CAD, USD, and some international currencies at airports based on the customer's instructions.<br>Brink's does not provide foreign exchange ("FX") services or FX rates. |
| Bitcoin ATM ("BATM")<br>• Pick-up<br>• Holding in treasury<br>• EFT to customer | In Scope | Brink's collects cash from BATMs and transports it to a processing centre (either Brink's or a third-party), and the funds go into treasury on behalf of the customer. Treasury services can be provided by Brink's or another third-party.<br>Alternatively, Brink's collects cash from BATMs and brings the cash back to a Brink's branch. Cash logistics process the cash, and the funds are then deposited into Brink's bank account. Brink's then transfers the funds to the customer's bank account via pre-authorized credit ("PAC").<br>Brink's only processes CAD based on the customer's instructions.<br>Brink's does not provide FX services or FX rates. |
| Cash Parcel Preparation ("CPP") | In Scope | Brink's CPP service handles cash deliveries exceeding CAD 10,000 per order, with amounts that can range in excess of CAD 500,000.<br>Brink's draws funds from the customer's bank account via pre-authorized debit ("PAD"). Cash parcels are prepared according to the customer's |

| | | |
|---|---|---|
| | | order with a lead time of six days to avoid customer transaction cancellations. After the lead time, the cash parcel is delivered by armoured truck to the customer.<br>These services are provided exclusively for cash parcels in CAD. |
| Change Fund Services – Brink's funded | In Scope | Change fund services refer to a service provided by Brink's to retailers, allowing customers to receive floats and rolls of coins directly at their business location saving them time and eliminating the need to travel to the bank.<br>Brink's customers can place orders through Brink's online system or Interactive Voice Response ("IVR") system. The customer's desired amount is taken from funds that are held in treasury at a Brink's location and delivered to the customer's business location.<br>Brink's offers change fund services with a delivery limit of CAD 3,000 per parcel. Funds are delivered through a courier service provider or Brink's armoured trucks.<br>For orders exceeding the CAD 3,000 limit, approval is obtained from the Brink's Controller. |
| Change Fund Services - CIT delivery – Bank funded | In Scope | Change fund services refer to a service provided by Brink's to retailers, allowing customers to receive floats and rolls of coins directly at their business location saving them time and eliminating the need to travel to the bank.<br>Brink's customers can place orders for change funds through Brink's online system or IVR system. Brink's draws cash directly from the customer's bank account via PAD. The collected cash is then brought to Brink's processing centre, where the Brink's cash logistics team prepares cash parcels based on the customer's requests.<br>The Company prepares and delivers the requested change fund parcels to the customer's business location.<br>Brink's armoured trucks deliver change funds to customers in conjunction with their CIT services. |
| Bank Parcel Pick Up - At Branch | In Scope | Brink's picks up cash from banks, whereby instead of the banks managing these funds directly, Brink's takes custody of the cash and holds it at the Company's own branches. This service is particularly aimed at two types of customers:<br>• Bank Orders (Contracted with Banks): This refers to agreements that Brink's has with banks to handle the physical movement and storage of cash. When banks need to manage large amounts of cash securely, they can rely |

| | | |
|---|---|---|
| | | on Brink's to pick up and store the funds until needed.<br>• ATM Operators: The ATM operators do not have to directly handle the logistics of transporting cash from banks to their own facilities; instead, Brink's manages this process for them.<br>Brink's has suspended this service for new customers, with the exclusion of requests initiated by a financial institution. |
| Brink's Complete - Advance Credit services (Brink's account) | In Scope | Brink's Capital Canada, a subsidiary of Brink's, offers the Brink's Complete Solution as part of the wider Digital Retail Solutions ("DRS"). Brink's Complete is a cash management service whereby the customer installs a Brink's tech-enabled device at their location. The customer is able to place currency in the device for credit to their bank account – this service is known as "Said -to-Contain EFT Claims". All currency placed in the device for credit is reported to Brink's Capital Canada (either by the customer themselves or via the smart safe) and such report constitutes the customer's request for credit to their bank account in the amount declared/reported. Once placed in the device, the ownership of the currency transfers to Brink's Capital Canada.<br>Once the cash is deposited, customers can also get real-time insights into their funds through Brink's customer portal.<br>Brink's (Brink's Canada Limited, not Capital) regularly collects the cash in the device and transports it to a Brink's Canada branch. At the branch, Brink's (Brink's Canada Limited, not Capital) processes and validates the cash against provisional credit records, reconciling any discrepancies through PAD and PAC. Once the cash is validated, it is placed into a separate, segregated Brink's Capital treasury held at the Brink's Canada branch. |
| CompuSafe - Advance Credit Services (Bank account) {Subcontracted CompuSafe} | In Scope | Brink's offers CompuSafe services to retail customers which is also a DRS solution. CompuSafes are smart safes with bill validators. CompuSafe allows customers to deposit cash safely into a secure safe. Through the Company's partnership with Canadian banks, mutual customers who are retailers, receive provisional credit from their bank for deposited cash through Brink's CompuSafe Advance Credit services.<br>Only Brinks personnel are authorized to open the CompuSafe once the customer deposits the cash. Brink's collects the cash deposits and transports them securely to a processing centre. The |

| | | |
|---|---|---|
| | | processing centre can be a Brink's facility, the bank's centre, or another ACC.<br>If Brink's is the processing facility, after validation and reconciliation, Brink's may hold the cash as treasury for the bank under a separate Cash Vaulting Service agreement with the bank or deliver it to the Canadian bank. |
| Low Volume Parcel ("LVP") | In Scope/Out of Scope[1] | Brink's BGS division provides LVP services to customers for shipping foreign currency, jewellery, and high-end clothing.<br>Only the shipping of foreign currency is covered by the PCMLTFA and is included in this RBA. Shipping jewellery and high-end clothing is out of scope of the PCMLTFA and is therefore not considered in this RBA.<br>This service is offered in partnership with a courier service provider for both business-to-business ("B2B") and business-to-customers ("B2C")[2]. Brink's provides an insured program that offers coverage above the courier service provider's insurance. |
| Precious Metal Storage (BGS) | Out of Scope[3] | BGS provides precious metal storage primarily for gold, silver, and palladium. Brink's picks up or delivers precious metals to and from refineries, mines, and other designated locations as directed by the customer. This portion of Brink's precious metals storage is not in scope for PCMLTFA and has not been considered as part of this RBA.<br>These metals can be bought, sold, and transported[4] between different customers.<br>For example: ABC bank sells gold bars to XYZ bank, Brink's will handle the logistics to move the gold from ABC bank's storage to XYZ bank's storage.<br>Brink's also offers pick and pack services where the Company stores coins for Dealers in Precious Metals and Precious Stones ("DPMS") customers. Upon receiving instructions from customers, Brink's packs and transports[5] these coins to the specified end user. |
| Valuable Transports (BGS) | In Scope/ Out of Scope[6] | Brink's provides secure transport services of high-value commodities including diamonds; jewellery; luxury goods; precious metals; negotiable |

[1] As of July 1, 2024, amendments to the PCMLTFA designate ACCs as reporting entities for transporting currency and negotiable instruments. However, the transportation and storage of precious metals, a common service provided by ACCs, is not included under these regulations at this time. Canada Gazette, Part 2, Volume 157, Number 21: Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act

[2] The provision of LVP services, specifically the transportation of foreign currency, is rare.

[3] See footnote 2.

[4] If Brink's is required to transport precious metals, the contract with the customer is under the Valuable Transports (BGS) services, not under the Precious Metal Storage (BGS) services contract.

[5] If transportation occurs, the contract with the customer is under the Valuable Transports (BGS) services, not under the Precious Metal Storage (BGS) services contract.

[6] As of July 1, 2024, amendments to the PCMLTFA designate ACCs as reporting entities for transporting currency and negotiable instruments. However, the transportation and storage of precious metals, a common service provided by ACCs, is not included under these regulations at this time. Canada Gazette, Part 2, Volume 157, Number 21: Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.

| | | |
|---|---|---|
| | | instruments like traveller's cheques, banks drafts, and money orders; stocks; bonds; certificates; currency; fine art; and other valuable assets.<br>Additionally, upon receiving instructions from its DPMS customers, Brink's packs and sends stored coins to the specified end user.<br>Only the shipping of currency (including coins and cash) and negotiable instruments like traveller's cheques, banks drafts, and money orders is covered by the PCMLTFA and is included in this RBA.<br>Shipping diamonds, jewellery, luxury goods, precious metals, stocks, bonds, certificates, fine art and other valuable assets that are not currency or negotiable instruments are out of scope of the PCMLTFA and is therefore not considered in this RBA.<br>These valuables are transported through armoured truck to the U.S. or through air transport internationally.<br>Brink's transports valuables directly from the owner to the owner's designated location allowing first-party transfers. Additionally, Brink's may also transport valuables on behalf of customers, but these transportation requests are always fulfilled on the instructions on the customer.<br>Occasionally, Brink's accepts requests for transporting precious metals through BGS for individuals. |
| Cash Vault Services | Out of Scope | Cash vault services are services generally offered to banks. These services can include treasury management, money processing, outgoing shipment preparation, cheque imaging, and certain reporting.<br><br>Brinks may hold foreign currency based on customer needs.<br>Since Bank of America ("BOA") does not have branches in Canada, in Toronto, Brink's acts as an agent of BOA and holds large volumes of USD.<br>Brinks provides vaulting services using Brink's system and network.<br>If any transportation is contemplated under these contracts with banks, it would be under a separate SOW and then fall under CIT above. |

Potential customers that are inquiring about Brink's services can fill out a business inquiry form on the Company's website. Customers are required to be fully onboarded prior to conducting transactions, which includes speaking with a Brink's sales representative, and submitting know-your-customer ("KYC") information through the online application form that is sent via a weblink. The Brink's compliance onboarding team reviews the application for validity and completeness and conducts additional due diligence measures as described in Section 9.1.

After the KYC is approved, the Company prepares a "Contract Agreement" and executes the Contract Agreement remotely via DocuSign or receives a wet signature in-person. The signed Contract Agreement outlines the specific services ordered, timeframes for the services, as well as the designated pick-up and drop-off locations including maximum amount limits.

Brink's customers can place additional orders outside of their existing contracts by contacting the sales team or customer service. These orders are then confirmed in writing via email. For Brink's change fund parcel service, customers place their orders through Brink's online system or IVR system. Customers can communicate with Brink's for customer support or general inquiries via telephone, email, and 24/7 mobile application.

The Company accepts payments via bank transfer, PAD, and cheque. Payments for BGS services can be received in USD. Transactions with customers are made via PAD, PAC, bank transfer, cash, and cheque. The Company utilizes banking partners in the course of providing services to customers.

At the time that this document was developed, Brink's did not utilize an agent network in the course of providing services to customers.[7]

All monetary values described in this document refer to the value in CAD unless otherwise noted.

[7] At the time this document was developed, Brink's was in the process of obtaining a policy interpretation from FINTRAC regarding the use of ground and air transportation services (for example, FedEx and commercial airlines) to determine if the use of these services qualifies as an agent relationship. The Company will update this document once FINTRAC has provided its interpretation.

# 1. Purpose

Brink's Canada Limited ("Brink's" or the "Company") is an armoured car company ("ACC") that is registered with the Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC"). On October 11, 2023, the federal government released the final version of the amendments to the Regulations under the Proceeds of Crime Money Laundering and Terrorist Financing Act ("PCMLTFA") in the Canada Gazette, Part II.[8] The newly released Regulations designate ACCs as reporting entities subject to the PCMLTFA and to be treated as a new category under the existing umbrella of money services businesses ("MSB"). The provisions in respect of ACCs will come into force on July 1, 2024.

[8] https://www.gazette.gc.ca/rp-pr/p2/2023/2023-10-11/pdf/g2-15721.pdf

## 2. Policy Application and Distribution

This AML Policy applies to all Brink's Canada Limited employees at offices wherever located.

This AML Policy is posted on Brink's intranet or otherwise made available to relevant employees. Brink's Canada Limited employees are required to review and understand the requirements of the Policy. In addition, this AML Policy is provided to all Brink's Canada Limited employees during initial and annual employee AML training.

## 3. Policy Administration

This AML Policy has been reviewed and approved by Brink's Canada Limited senior management, responsible for the final approval of this AML Policy and oversight of the AML Program. Any material revisions to this Policy require approval by Brink's Canada Limited senior leadership.

Brink's Canada Limited AML Officer owns this policy and is responsible for its issuance, maintenance, and interpretation. The AML Officer will, at a minimum, annually review this policy as required.

# 4. Glossary

The following is a list of abbreviations and definitions used throughout this document:

| Term | Definition |
|---|---|
| **AML** | Anti-money laundering |
| **CDD** | Customer due diligence |
| **CSIS** | Canadian Security Intelligence Service |
| **CTF** | Counter-terrorism financing |
| **EDD** | Enhanced due diligence |
| **EFT** | Electronic funds transfer |
| **Entity** | A corporate body, trust, partnership, fund, or an unincorporated association or organization. |
| **Final Receipt** | The receipt of the instructions by the person or entity that is to make the remittance to the beneficiary. |
| **Financial Institution** | For the purpose of this document, financial institution refers to a bank, credit union, caisse populaire, or building society. |
| **FINTRAC** | Financial Transactions and Reports Analysis Centre of Canada |
| **HIO** | Head of an international organization |
| **Initiation** | The first transmission of the instructions for the transfer of funds. |
| **KYC** | Know your customer |
| **Money Laundering ("ML")** | Dealing with property or the proceeds of property with the intent to conceal or convert it, knowing, believing or being reckless as to whether it was obtained or derived from the commission of an indictable offence. Concealment is not necessary for an offence and conversion can be as simple as a deposit or a transfer. |
| **PCMLTFA** | Proceeds of Crime (Money Laundering) and Terrorist Financing Act |
| **PEP** | Politically exposed person |
| **PIN** | Purpose and intended nature |
| **Proceeds** | Proceeds refers to any property derived from or obtained, directly or indirectly, through the commission of an offence. |
| **Program** | Policy Manual, Compliance Regime, Regime, or Program: the set of policies and procedures laid out in this document that apply to all employees including contractors, consultants, partners, professional employees, students, and all related subsidiaries and entities. |
| **RCMP** | Royal Canadian Mounted Police |
| **Reasonable Measures** | Steps taken to achieve a desired outcome, even if they do not result in the desired outcome. For example, this can include doing one or more of the following:<br>• asking the customer,<br>• conducting open-source searches,<br>• retrieving information already available, including information held in non-digital formats, or<br>• consulting commercially available information. |
| **Senior Management** | For the purposes of this Program, Brink's Canada Limited's Senior Management consists of the following:<br>• Executive Vice-President and General Counsel of The Brink's Company and Vice President of Brink's Canada Limited;<br>• Vice-President of Digital Solutions and Director of Brink's Canada Limited;<br>• Sr. Vice-President of Finance and Admin.;<br>• Sr. Director of Risk Management and Corporate Security;<br>• Vice-President of Field Operations;<br>• Vice-President of BGS Latin America and Canada; and<br>• Vice-President, AML and Sanctions Compliance Officer ("Compliance Officer"). |
| **STR** | Suspicious transaction report |
| **Structuring** | Structuring is a common money laundering methodology where transaction sizes are deliberately selected to avoid triggering identification or reporting requirements. |
| **Terrorist** | The term terrorist refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organizes or directs others to commit terrorist acts ; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common |

| | |
|---|---|
| | purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act. |
| **Terrorist Act** | A terrorist act includes:<br>a) an act which constitutes an offence within the scope of, and as defined in one of the following treaties: (i) Convention for the Suppression of Unlawful Seizure of Aircraft (1970); (ii) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971); (iii) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973); (iv) International Convention against the Taking of Hostages (1979); (v) Convention on the Physical Protection of Nuclear Material (1980); (vi) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988); (vii) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation ( 2005); (viii) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (2005); (ix) International Convention for the Suppression of Terrorist Bombings (1997); and (x) International Convention for the Suppression of the Financing of Terrorism (1999).<br>b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act. |
| **Terrorist Financing ("TF")** | Terrorist financing is the financing of terrorist acts, and of terrorists and terrorist organizations. |
| **Terrorist Organization** | The term terrorist organization refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organizes or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act. |
| **TPR** | Terrorist property report |
| **UTR** | Unusual transaction report |
| **VSDONC** | Voluntary self-declaration of non-compliance |

# 5. Regulatory Framework

Canada has a national framework in place to detect and deter money laundering ("ML") and terrorist financing ("TF") and aid in the identification, investigation, and prosecution of ML/TF offences. Similarly, provinces may enact prudential sector-specific regulations to manage a variety of risks, including those that relate to ML/TF offences. This section sets out the various applicable laws and regulations that have been enacted as they relate to ML/TF, collectively referred to as the "Legislation" throughout this document.

## 5.1 PROCEEDS OF CRIME (MONEY LAUNDERING) AND TERRORIST FINANCING ACT

In December 2001, Canada enacted the Proceeds of Crime (Money Laundering) and Terrorist Financing Act ("PCMLTFA") that makes it mandatory for various individuals and entities ("Reporting Entities") to implement a compliance program that meets the requirements set out in the Legislation.

The PCMLTFA also established FINTRAC as the agency responsible for the collection, analysis, and disclosure of information to assist in the detection, prevention, and deterrence of

ML/TF activities in Canada and abroad. FINTRAC is Canada's financial intelligence unit and fulfils its mandate through:

- receiving financial transaction reports and voluntary information in accordance with the PCMLTFA;
- ensuring compliance of reporting entities with the PCMLTFA;
- producing financial intelligence relevant to ML/TF and threats to the security of Canada;
- researching and analyzing data on trends and patterns in ML/TF;
- maintaining a registry of MSBs in Canada; and
- enhancing public awareness and understanding of ML/TF activities.

Towards the achievement of its mandate of ensuring compliance with the PCMLTFA, FINTRAC conducts examinations of Reporting Entities.

FINTRAC is authorized to levy administrative monetary penalties against Reporting Entities that fail to implement effective compliance programs, and to recommend instances of criminal non-compliance for prosecution.

## 5.2 MONEY SERVICES BUSINESS ACT – QUÉBEC

The province of Québec has enacted the Money Services Business Act ("MSBA"), as well as associated regulations, applicable to MSBs operating in the province of Québec.

Revenu Québec administers oversight of the MSBA and is empowered to conduct examinations and issue sanctions for contraventions of the MSBA.

At the time this document was developed, the Company did not provide MSB services or have offices in the province of Québec. As such, the Company is not required to register with, or obtain a licence from, Revenu Québec

## 5.3 MONEY SERVICES BUSINESS ACT – BRITISH COLUMBIA

The province of British Columbia ("B.C.") has enacted the Money Services Business Act ("MSB Act") on March 29, 2023, requiring MSBs operating in the province of B.C. to register with the B.C. Financial Services Authority ("BCFSA"). The Act received Royal Assent on May 19, 2023; however; the regulations related to the B.C. MSB Act have yet to be published. There has been no timeline published as to when to expect the regulations.

Under this new legislation, the BCFSA will appoint a new Superintendent of MSBs who will become the primary provincial regulator of MSBs.

The Company will continue to monitor the development of the B.C. MSB Act and regulations, and will make the necessary updates to this document once the regulations have been finalized.

## 5.4 ECONOMIC SANCTIONS LAWS AND REGULATIONS

Canada's legislative measure against terrorists, terrorist groups, and other listed and sanctioned individuals and entities are contained in various Canadian statutes and regulations, or those adopted by Canada, including the Criminal Code of Canada, United Nations Act, Justice for the Victims of Corrupt Foreign Officials Act ("Sergei Magnitsky Law"), and the Special Economic Measures Act ("SEMA").

These regulations are applicable to all individuals and entities conducting business in Canada as well as all Canadian citizens and Canadian incorporated businesses operating outside of Canada.

The Department of Foreign Affairs, Trade, and Development and the Department of Public Safety Canada are responsible for administering the statutes and regulations within Canada.

For the purposes of this document, a "Designated Person" is any person or entity listed on a government created list, or one created by a relevant regulatory body, of those individuals or entities associated with or suspected of being associated with terrorism. Specific measures vary depending on the relevant legislation, but broadly include:

- prohibitions in dealing with property owned or controlled by Designated Persons;
- prohibitions on providing any financial or related services in respect of property owned or controlled by Designated Persons; and
- prohibitions on entering or facilitating transactions with, or making available property or financial services to, Designated Persons.

## 5.5 COMPLIANCE WITH THE LEGISLATION

On October 11, 2023, the Department of Finance released the final version of the regulations amending the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations ("PCMLTFR" or the "Regulations") to include the armoured car sector as a category of MSB activities under the PCMLTFA[9]. According to the released Regulations, those engaged in "transporting currency or money orders, traveller's cheques or other similar negotiable instruments except for cheques payable to a named person or entity" will be classified as a new category of MSB.[10]

Under the Regulations, Brink's is, therefore, considered to be an MSB, as defined in section 5(h.1) of the PCMLTFA, because the entity provides transportation services for currency as well as negotiable instruments. As such, it is considered a Reporting Entity with obligations to meet all the requirements specified by the Legislation.

To comply with the Regulations, Brink's has implemented an AML/CTF compliance program that aligns with the regulatory obligations specific to MSBs.

The Legislation imposes certain responsibilities on Reporting Entities when they conduct transactions. Those responsibilities include, but are not limited to:

- identifying customers in prescribed circumstances;
- keeping records about their transactions;
- monitoring business relationships; and
- reporting prescribed transactions to FINTRAC.

### 5.5.1 PENALTIES AND CONSEQUENCES OF NON-COMPLIANCE

The failure of a Reporting Entity to implement and adhere to an effective compliance program can expose it to serious regulatory intervention and potentially affect its ability to conduct business. If FINTRAC observes compliance failures, it has the option to:

[9] https://www.gazette.gc.ca/rp-pr/p2/2023/2023-10-11/pdf/g2-15721.pdf
[10] https://lois-laws.justice.gc.ca/eng/acts/P-24.501/FullText.html

- apply monetary penalties, which range from $1,000 per violation to $500,000 per violation based on the severity of the failure; or
- refer offences for criminal prosecution with potential fines up to $2 million and/or imprisonment for up to five years.

The PCMLTFA Administrative Monetary Penalties Regulations provide guidance on the severity of violations. The largest penalties and fines are reserved for instances where a Reporting Entity or those involved in its activities fail to report a suspicious transaction. For example, FINTRAC may levy a penalty of $1,000 for every failure to properly identify a customer, and $500,000 for every failure to file a suspicious transaction report ("STR") or terrorist property report ("TPR").

Directors and officers can be subject to prosecution if they direct, authorize, assent to, acquiesce, or participate in the commission of the compliance offence of a Reporting Entity, while employees can be subject to criminal prosecution if they fail to report suspicious transactions, unless the transaction has been reported to their supervisor.

No criminal or civil proceedings may be brought against a person for making a report in good faith concerning a suspicious transaction.

Economic sanctions are generally enforced by the Royal Canadian Mounted Police ("RCMP") and offences can result in fines of up to $100,000 and/or imprisonment.

## 6. Policy Objectives

This policy is written to express the commitment of Brink's to comply with prevailing anti-money laundering ("AML")/counter-terrorism financing ("CTF") obligations under the Legislation.

This policy formalizes roles and responsibilities across the Company with respect to these requirements with a view to helping the Company reduce legal, regulatory, financial, and reputational risk. This policy is designed to ensure that all applicable regulatory requirements are met and, as such, it is imperative that management and any employees consistently adhere to the contents herein.

Brink's Senior Management that forms the Brink's Canada Compliance Committee consists of the following:

- Executive Vice-President and General Counsel of The Brink's Company and Vice President of Brink's Canada Limited;
- Vice-President of Digital Solutions and Director of Brink's Canada Limited;
- Sr. Vice-President of Finance and Admin.;
- Sr. Director of Risk Management and Corporate Security;
- Vice-President of Field Operations;
- Vice-President of BGS Latin America and Canada; and
- Vice-President, AML and Sanctions Compliance Officer ("Compliance Officer").

This policy has been reviewed and authorized by Senior Management, and a signed record of that approval is maintained for compliance purposes.

## 7. MSB Registration, Licensing, And Renewal

## 7.1 FINTRAC REGISTRATION AND RENEWAL

As an MSB, Brink's is required to register with FINTRAC and keep its registration information up to date. The Company's FINTRAC MSB registration number is C100000030.

Changes to Brink's registration information must be submitted to FINTRAC no later than 30 days after any of the following changes:

- MSB services offered;
- information about financial accounts used to provide MSB services;
- information about other Canadian MSBs that Brink's uses to conduct transactions;
- information about the Company's Compliance Officer;
- incorporation information (name, registered address, etc.);
- information about the Company owners and directors, including but not limited to name and date of birth; and
- detailed information about every branch and/or agent.[11]

It is the responsibility of Brink's Compliance Officer to keep the registration information up to date. The Compliance Officer reviews Brink's registration monthly to determine if there are any material changes that require an update to the registration.

The Compliance Officer is required to renew its registration every two years prior to expiry. Brink's current registration expires on 2026-07-31.

At the time of the registration renewal, the Compliance Officer also updates the number of individuals that Brink's employs, as well as the estimated annual transaction value.[12]

## 7.2 MONEY SERVICES BUSINESS ACT – BRITISH COLUMBIA

As there are no regulations in place in B.C. at the time this document was developed, there are no registration requirements.

The Company continues to monitor the development of the B.C. MSB Act and regulations and will make the necessary updates to this document once the regulations have been finalized.

# 8. AML/CTF COMPLIANCE PROGRAM

To ensure compliance with the Legislation, Reporting Entities are required to develop, apply, and maintain a compliance program (the "Program"). This document addresses the following elements of the Program:

- Written compliance policies and procedures;
- The appointment of a designated Compliance Officer;
- Risk-based assessment and management plan;
- An ongoing training program; and
- Periodic compliance effectiveness reviews.

[11] At the time that this document was approved, the Company operated from a registered office located in Etobicoke, Ontario. At the time this document was developed, Brink's was in the process of obtaining a policy interpretation from FINTRAC regarding the use of ground and air transportation services (for example, FedEx and commercial airlines) to determine if the use of these services qualifies as an agent relationship. The Company will update this document once FINTRAC has provided its interpretation.

[12] A change in the expected dollar amount of transactions would represent an increase of 30% or more in the total transaction volume over the course of the year following renewal.

## 8.1 POLICIES AND PROCEDURES

Brink's has developed written policies and procedures that meet the requirements set out in the Legislation for MSBs. These policies and procedures are an important component of Brink's Program as they guide the Company's decisions and actions with respect to the implementation of the Program.

The Company's compliance policies and procedures are:

- written and maintained in a form/format that is accessible to all employees;
- periodically reviewed and updated to reflect changes in the Legislation, changes in operations, or identified regulatory gaps; and
- approved by Senior Management.

Brink's written policies and procedures outline all obligations, corresponding processes, and controls applicable under the Legislation, including:

- development and maintenance of the Program;
- customer identification and other due diligence;
- ongoing monitoring and other responsibilities relating to business relationships;
- maintenance of required records; and
- the reporting of prescribed transactions to FINTRAC.

Brink's written policies and procedures also address how the Company handles ministerial directives and transaction restrictions, which are targeted measures issued by the Minister of Finance to protect Canada's financial system from being used for ML/TF purposes.

## 8.2 APPOINTMENT OF A DESIGNATED COMPLIANCE OFFICER

Brink's has appointed a designated Compliance Officer who is responsible for the implementation and maintenance of the Program. The Compliance Officer is provided with unfettered access to all pertinent information and records.

A back-up Compliance Officer may also be designated during times when the Compliance Officer is absent. In the absence of the Compliance Officer, the back-up Compliance Officer has the same responsibilities and authority as the Compliance Officer.

The Compliance Officer may choose to delegate certain duties. However, where such a delegation is made, the Compliance Officer retains overall responsibility for the implementation of the Program.

The Company must maintain the appointment of a Compliance Officer. When a vacancy occurs, Brink's ensures that the appointment of a new Compliance Officer occurs immediately. It is the responsibility of Senior Management to maintain the appointment of a Compliance Officer.

The appointment of Brink's Compliance Officer is documented in Appendix A.

### 8.2.1 RESPONSIBILITIES OF THE DESIGNATED COMPLIANCE OFFICER

The Compliance Officer is responsible for the direction of the Program, and for ensuring that all existing and future employees and business affiliates of the Company adhere to the policy and procedural standards outlined in this document.

The Compliance Officer is responsible for:

- ensuring compliance with the Company's Program;
- providing timely inherent risk analysis and ensuring that the Program is current and relevant to identified risks;
- ensuring written AML/CTF policies and procedures are kept up to date;
- assessing the adequacy of system resources, including those required to identify and report suspicious and attempted suspicious transactions;
- ensuring that an adequate training program is implemented, and that the training program is periodically reviewed and updated;
- ensuring that the Program undergoes a periodic effectiveness review that meets the standards set out in the Legislation;
- ensuring that all employees follow documentation retention requirements;
- acting as the principal point of contact for communication with regulatory authorities;
- responding to requests for information from regulatory authorities in a timely manner, and ensuring that FINTRAC requests are responded to within 30 days of the request;
- ensuring that reportable transactions are reported to FINTRAC, within the mandated timeframe; and
- ensuring that customer due diligence ("CDD") and enhanced due diligence ("EDD") is conducted as required by Brink's policy.

The Compliance Officer at Brink's is a member of the Senior Management team and provides quarterly reports to other members of the Senior Management team with respect to:

- customers who have been identified as high risk;
- reports that have been submitted to FINTRAC;
- any incidents of non-compliance; and
- significant changes identified in Brink's ML/TF risks.

## 8.3 RISK-BASED ASSESSMENTS AND MANAGEMENT

Brink's uses a risk-based approach to assess the risks related to ML/TF, as well as to document and implement mitigating controls to address those risks.

Brink's risk assessment and methodology were developed in accordance with FINTRAC's guidance on the risk-based approach, Financial Action Task Force ("FATF") recommendations, and with consideration of industry sources and best practices to assess the ML/TF risks related to:

- geographies of the Company's operations;
- services/access channels the Company provides to its customers, including those based on new and developing technologies;
- customer relationship characteristics; and
- other relevant factors (where applicable).

The risk assessment and methodology are maintained by the Compliance Officer in a separate document, titled Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) Risk-Based Approach Methodology (the "Risk Assessment") and are to be used in day-to-day operations to assess the level of risk that a particular business relationship or individual transaction presents and to apply the relevant controls.

The Risk Assessment takes into consideration the inherent risk of business activities and customer relationships, where inherent risk is the intrinsic risk of an event or circumstance that exists before the application of controls or mitigation measures. For areas that have been

identified as being high risk, controls or measures have been implemented to mitigate the identified risk, including conducting enhanced ongoing monitoring and keeping customer information up to date. See the Risk Assessment for more information.

The Compliance Officer is responsible for ensuring that the Risk Assessment is kept up to date and reviewed at least every two years, or when there are changes to assessed risk factors (e.g., the addition of new products or services). A record of reviews and changes is maintained by the Compliance Officer.

### 8.3.1 ENHANCED DUE DILIGENCE

Brink's applies EDD measures when a customer is determined to be high risk. Measures are designed to mitigate the specific risks posed by each high-risk customer.

The minimum EDD measures conducted for each type of high-risk customer are defined in the Company's Risk Assessment. The Compliance Officer may, however, apply any additional measure(s) that they determine is required to sufficiently mitigate a customer's risk.

### 8.3.2 DERISKING OF HIGH-RISK CUSTOMERS

There are certain circumstances that fall outside of Brink's risk tolerance. In these circumstances, the Company is prohibited from onboarding new customers. In the case of existing customers, Brink's policy is to de-risk the customer and not conduct any further transactions.

Determination of whether a customer should be de-risked is within the sole discretion of Senior Management.

Refer to Brink's Risk Assessment for a detailed listing of the circumstances that trigger the Company's de-risking policy.

## 8.4 TRAINING PROGRAM

Brink's aims to recruit, attract, and retain employees who are qualified, competent, and ethical.

To ensure employees understand the Company's reporting, customer identification, and recordkeeping requirements, Brink's has documented a training program and provides training to all employees that:

- have direct contact with customers;
- assist in processing or monitoring customer transactions;
- handle funds in any way; and/or
- are responsible for implementing or overseeing the Program.

Brink's training program is designed to ensure employees and those authorized to act on behalf of the Company receive compliance training that meets the standards set out by the Legislation.

Training content is reviewed, and updated, if necessary, by the Compliance Officer, at a minimum of every two years, but may be updated more frequently as required.

Ongoing training may be provided in the form of PowerPoint presentations, in-house presentations by the Compliance Officer, departmental discussions, online presentations, guest

speakers, or written presentations. Training may be produced and/or conducted by an external agency, as appropriate.

Brink's maintains records of all training activities including, but not limited to:

- trainee name;
- date of hire;
- type of training delivered;
- date of training delivery; and
- date of training completion.

See Appendix B for a sample training log.

### 8.4.1 EMPLOYEE TRAINING

Employees and those authorized to act on behalf of the Company receive appropriate training prior to dealing with customers, as it applies to their role. Training is provided within 90 days of hiring with refresher training provided, at least, annually thereafter.

The Company may exempt an authorized person acting on behalf of the Company from Brink's training program, where it can be demonstrated through a review of training materials, independent evaluation, or certification of their training program that the person obtains training that is equivalent to what would be required if acting in the same capacity as an employee.

Training content is intended to ensure that employees of the Company and those authorized to act on behalf of the Company are aware of and understand:

- their requirements under the PCMLTFA and associated Regulations;
- background information on ML/TF, such as the definition of ML/TF and methods of ML/TF;
- how the Company's business could be vulnerable to ML/TF activities (provide indicators and examples);
- the Company's compliance policies and procedures to help meet the requirements under the PCMLTFA and associated Regulations for preventing and detecting ML/TF, including reporting, record keeping and KYC requirements; and
- their roles and responsibilities in detecting and deterring ML/TF activities, and when dealing with potentially suspicious activities or transactions.

At the completion of initial and refresher training, the Company administers a knowledge assessment quiz, and trainees are required to obtain a minimum score of 80%. Re-tests are given to those trainees who do not pass the test on the first attempt. Trainees who fail to obtain a score of 80% or higher on their second attempt receive remedial training.

Quiz results are retained by the Compliance Officer and are available upon request.

Compliance staff are required to take supplemental training with respect to:

- reporting obligations;
- conducting investigations of suspicious activity;
- suspicious transaction reporting; and
- terrorist property reporting.

### 8.4.2 COMPLIANCE OFFICER TRAINING

The Compliance Officer maintains an in-depth knowledge of the Legislation by attending facilitated training sessions and/or through a self-study program. The Compliance Officer stays informed of legislative changes by means of reviewing information circulated from various sources, or from gaining access to information published by FINTRAC and/or other related government associations.

Additionally, Brink's requires the Compliance Officer to attend at least one annual in-person or virtual training, conference, seminar, or webinar on compliance or financial crime matters.

### 8.4.3 SENIOR MANAGEMENT TRAINING

The Compliance Officer ensures that Senior Management receives appropriate training, as it applies to their role, as part of their orientation, and at least annually thereafter.

Training is sufficient so that Senior Management is able to manage the oversight responsibility they are mandated with. The training includes topics such as:

- roles and responsibilities of Senior Management, employees, and the Company, including any statutory obligations;
- sufficient briefing with inherent risks and controls to enable Senior Management to assess information reported by the Compliance Officer and auditors;
- penalties, fines, and potential imprisonment associated with non-compliance; and
- emerging trends and methodologies.

Where Senior Management is involved in day-to-day compliance, supplementary training that is relevant to their business area is provided.

The Compliance Officer may choose to provide the training via one-on-one sessions, in groups, through electronic training, or by written communication distributed to appropriate parties.

## 8.5 EFFECTIVENESS REVIEW

An independent effectiveness review of the Program is conducted at a minimum of every two years and must begin within two years of the start date of the previous review. The Company may conduct the review internally (as long as the review is conducted by someone who is not directly involved in compliance program activities), or it may outsource the conduct of the review to an external firm. The reviewer must be sufficiently qualified and possess appropriate knowledge of the Company's ML/TF risks, controls, and relevant threats and requirements.

The effectiveness review is conducted with a view to identifying areas where the Program may require updating, where there are weaknesses in its design and/or implementation, and/or where there are lapses in compliance with respect to the Legislation. Where necessary, the Compliance Officer must design an action plan to remediate any deficiencies, identifying the parties responsible for implementing the changes, and a timeline for remediation. The Compliance Officer ensures any required changes or updates to the information are appropriately communicated.

The reviewer evaluates the Program against existing standards and performs a series of tests on the effectiveness of its implementation. Testing is done on a sample basis and addresses all areas of the Program.

The results of the effectiveness review must be reported in writing to a senior officer no later than 30 days after the completion of the review. The report must include:

- the findings of the review, including deficiencies identified, planned corrective actions, implementation timeline, etc.;
- any updates that were made to the policies and procedures during the reporting period; and
- the status of the implementation of the updates made to the policies and procedures.

Brink's Compliance Officer is a senior officer and, therefore, has immediate access to drafts and final versions of the effectiveness review report, including the documented response as outlined above, and therefore the 30-day timeline is met by virtue of the process design.

# 9. Know Your Customer Obligations

Brink's acknowledges the importance of implementing appropriate KYC controls and procedures to identify its customers, develop customer profiles, and understand expected transactions in such a way as to diminish its legal, financial, and reputational risk.

Furthermore, whenever engaging in activities governed by the PCMLTFA, known as "Qualifying Activities," the Legislation imposes certain requirements such as identification, recordkeeping, and reporting when performing prescribed transactions.

This section outlines the policies and procedures with respect to customer identification, business relationships, ongoing monitoring, third-party determinations, and customer screening.

## 9.1 CUSTOMER INFORMATION COLLECTION

Potential customers that are inquiring about Brink's services can fill out a business inquiry form on the Company's website by providing the following information:

- First and last name;
- Email address;
  - Phone number;
  - Company name;
  - Address;
  - City;
  - Province;
  - Postal code;
  - Selecting their desired business product/service;

Customers are required to be fully onboarded prior to conducting transactions, which includes completing the below steps in the following order:

- Speaking with a Brink's sales representative either via telephone or in-person to discuss the specifics of their business needs and confirming a new contract; and
- Completing and submitting an online application form shared through a weblink via email by the Brink's sales team which includes the following information:
  - Company name;
  - Trade name;
  - Telephone number;
  - Business address including city, province, country and postal code;[13]

[13] The office address must be a physical address. A P.O. Box is not acceptable for the purpose of complying with the Legislation.

- Nature of principal business (see Section 14.2);
- Company incorporation/registration details;
- Website;
- Company structure;
- Entity type;
- GST/HST registration details;
- Description of services required;
- Service frequency;
- Value of shipments;
- Banking information including branch, account number, telephone number, and address;
- Method of payment;
- Trade references;
- The following information for authorized signors:
  - Full name;
  - Date of birth;
  - Residential address;
  - Job title;
- The following information for each authorized employee:
  - Full name;
  - Date of birth;
  - Residential address;
  - Job title;

- Submitting all supporting documents related to KYC as applicable to the entity type.

When an application is received, the compliance onboarding team is notified via email. The compliance onboarding team reviews the customer's submitted information for validity and completeness. Additionally, the Company verifies the identity of customers, as well as the officers, directors, authorized employees, and beneficial owners[14] (collectively "Principals"), as described in Section 9.3, and conducts a third-party determination as described in Section 9.4.

The Company conducts watchlist screening, including sanctions and adverse media checks, on customers and the Principals of entity customers at onboarding and periodically thereafter. Brink's also conducts watchlist screening, including sanctions, adverse media checks, on beneficiaries at the time of the transaction. Politically exposed person ("PEP")/head of an international organization ("HIO") screening is conducted on individual customers and the Principals of entity customers at onboarding and periodically thereafter. See Section 9.6 for a more detailed description of the customer screening process.

Once customer KYC is reviewed and approved by the compliance team, a "Contract Agreement" is built and sent to the customer for execution via DocuSign or a wet signature.

The Company conducts EDD measures consistent with the Company's Risk Assessment to ensure that enhanced measures are put in place for high-risk customers, as described in the Risk Assessment.

## 9.2 QUALIFYING ACTIVITIES

The following describes the Qualifying Activities and corresponding regulatory obligations triggered by those activities, based on the Company's current business model. These include:

[14] As a standard, the Company verifies beneficial owners who own or control 25% or more shares of the customer.

- Transportation of $1,000 or more in cash;
- Transportation of $3,000 or more in money orders, traveller's cheques, or other similar negotiable instruments;
- Large cash transactions ("LCT");
- Customer information records for Service Agreements; and
- Suspicious transactions and attempted suspicious transactions.

As a policy, the Company collects information as described in Section 9.1. The same information does not need to be collected again as a result of the regulatory obligations related to qualifying activities described in this section.

### 9.2.1 TRANSPORTATION OF $1,000 OR MORE IN CASH

If Brink's transports $1,000 or more in cash, the Company is required to take the following actions:

- verify the identity of the individual or entity conducting the transaction prior to the first transaction taking place (see Section 9.3);
- obtain the name, address, date of birth (for individuals), and occupation/nature of principal business (see Section 14.2) for any person or entity that made the request;
- obtain the name and address, if known, of each beneficiary; and
- maintain a record of the transaction (see Section 14).

### 9.2.2 TRANSPORTATION OF $3,000 OR MORE IN MONEY ORDERS, TRAVELLER'S CHEQUES, OR OTHER SIMILAR NEGOTIABLE INSTRUMENTS

If Brink's transports $3,000 or more in money orders, traveller's cheques, or other similar negotiable instruments (except for cheques payable to a named person or entity), the Company is required to take the following actions:

- verify the identity of the individual or entity conducting the transaction prior to the first transaction taking place (see Section 9.3);
- obtain the name, address, date of birth (for individuals), and occupation/nature of principal business (see Section 14.2) for any person or entity that made the request;
- obtain the name and address, if known, of each beneficiary; and
- maintain a record of the transaction (see Section 14).

### 9.2.3 LARGE CASH TRANSACTIONS

An LCT occurs when all cash received from or on behalf of the same individual or entity for transport totals more than $10,000 or more or the equivalent value in a foreign currency within the Company's 24-hour period (see Section 11.1).

When Brink's conducts an LCT, the Company is required to take the following actions:

- verify the identity of the individual conducting the transaction at the time that the transaction takes place (see Section 8.3);
- obtain the name, address, date of birth, and occupation/nature of principal business for any person or entity that made the request;
- make a third-party determination (see Section 8.4);
- submit a large cash transaction report ("LCTR") to FINTRAC (see Section 11.5); and
- maintain a record of the LCT (see Section 13).

### 9.2.4 LARGE CASH TRANSACTIONS

As a policy, Brink's enters into a Service Agreement also known as a "Contract Agreement" with all entity customers.

A Service Agreement is an agreement between the customer and Brink's, under which Brink's provides cash transportation; transportation of money orders, traveller's cheques, or other negotiable instruments; BATM cash pick-up; fiat ATM cash pick-up and replenishment services, as well as additional services on an ongoing basis.

Upon entering into a Service Agreement, a customer information record is created and maintained by the Company. An information record is a record that contains the name, address, and nature of the entity's principal business (see Section 14.2).

When creating a customer information record, the Company also takes reasonable measures to determine if the entity is or will be conducting transactions on behalf of a third party, as described in Section 9.4. When entering into a Service Agreement, the following additional information is collected:

- Record of those who signed the Service Agreement – name, address, date of birth, and occupation of every individual who signed the Service Agreement on behalf of the entity; and
- List of authorized employees[15] – name, address, and date of birth of every employee of the entity who is authorized to order transactions under the Service Agreement.

For entities that are corporations, if in the normal course of operations, the Company obtains a copy of the part of the official corporate records showing the provisions that relate to the power to bind the corporation regarding transactions (e.g., certificate of incumbency, articles of incorporation, or the bylaws of the corporation that set out the officers duly authorized to sign on behalf of the corporation, etc.), a record of those documents is maintained. If there were changes subsequent to the articles or bylaws that relate to the power to bind the corporation regarding the transactions and these changes were applicable at the time the customer information record was created, then the board resolution stating the change would be included in this type of record.

At the time the Company creates a customer information record, Brink's must also verify the identity of the entity, as described in Section 9.3.

### 9.2.5 SUSPICIOUS TRANSACTIONS AND ATTEMPTED SUSPICIOUS TRANSACTIONS

Brink's takes reasonable measures to identify individuals and entities who conduct or attempt to conduct a suspicious transaction before submitting an STR to FINTRAC, including a transaction that might otherwise be exempted from customer identification requirements.

Reasonable measures in this case may include asking the individual or entity to provide identification information used to verify their identity as set out in Section 9.3.

Brink's does not have to take reasonable measures to identify the individual or entity who conducts or attempts to conduct a suspicious transaction if:

[15] The Company does not have to obtain information on persons authorized to provide instructions where a Service Agreement is signed for the transportation of cash with the Bank of Canada, with two financial entities, or between two places of business of the same entity.

- the Company has already verified the individual or entity's identity as required in Section 9.3 and has no doubts about the identification information; or
- Brink's believes verifying the individual or entity's identity would inform them that the Company is considering submitting an STR.

For more information on identifying, investigating, and reporting suspicious transactions, see Section 12.3.

## 9.3 CUSTOMER IDENTITY VERIFICATION

This section outlines the policies and procedures with respect to verifying identity. In all cases, employees are responsible for ensuring individuals are appropriately identified using authentic, valid, and up-to-date information.

### 9.3.1 GENERAL EXCEPTION TO IDENTITY VERIFICATION

Brink's is not required to verify the identity of a person or an entity in respect of the transportation of coins of the currency of Canada that are produced or supplied by the Royal Canadian Mint that are delivered to the Minister of Canada (or to a person designated by the Minister of Finance).

Brink's is not required to verify the identity of a person or an entity in respect of the transportation of cash, money orders, traveller's cheques, or other similar negotiable instruments between:

- the Bank of Canada and a person or entity in Canada;
- two financial entities; or
- two places of business of the same reporting entity, other than a request made by another person or entity.

The Company does not have to re-identify a customer if it previously did so using the methods specified in the Legislation in place at the time, and the relevant records were kept, so long as there are no doubts about the information used to verify the identity.

Brink's does not have to verify the identity of an authorized employee who conducts a transaction for their employer under a Service Agreement.

Brink's does not have to verify the names of directors when verifying the identity of a corporation that is a securities dealer.

The Company is not required to verify the identity of an entity or obtain and confirm beneficial ownership information of a public body or a very large corporation[16]. The same is true regarding a subsidiary of either of those entities, if the financial statements of the subsidiary are consolidated with those of the public body or very large corporation.

Notwithstanding, the Company does obtain and keep a copy of the official records showing the provisions that relate to the power to bind the corporation, such as a certificate of incumbency, the articles of incorporation, or the bylaws of the corporation or subsequent

[16] A very large corporation or trust that has minimum net assets of $75 million on its last audited balance sheet, whose shares or units are traded on a Canadian stock exchange or a stock exchange designated under subsection 262(1) of the Income Tax Act and that operates in a country that is a member of the FATF.

board resolutions that set out the officers duly authorized to sign on behalf of the corporation, such as the president, treasurer, vice-president, comptroller, etc.

### 9.3.2 VERIFYING THE IDENTITY OF AN INDIVIDUAL

When Brink's is required to verify the identity of an individual customer, as well individuals associated with an entity customers such as an entity customer's Principals, the Company uses the government photo ID method.

Brink's relies on valid, current, and authentic photo identification documents ("ID"), issued by a federal, provincial, or territorial government to verify the identity of an individual. An ID issued by a municipal government (either Canadian or foreign) is not acceptable.

Brink's does not accept an ID when:

- it does not indicate the individual's name, or the name that the individual provided does not match the name appearing on the ID;
- it does not have a photo, or the photo on the ID provided does not match the likeness of the individual presenting it;
- the ID does not have a unique identifier; or
- the ID is expired.

The following is a list of acceptable IDs.

| **Acceptable ID** |
|---|
| • Driver's Licence<br>• Passport<br>• Permanent Resident Card<br>• Secure Certificate of Indian Status<br>• British Columbia Services Card<br>• Firearms Licence<br>• Provincial or territorial health card, where not prohibited by provincial legislation[17]<br>Provincial or territorial identification card issued by:<br>• Insurance Corporation of British Columbia<br>• Alberta Registries<br>• Saskatchewan Government Insurance<br>• Department of Service Nova Scotia and Municipal Relations Department of Transportation and Infrastructure Renewal of the province of PEI<br>• Service New Brunswick<br>• Department of Government Services and Lands of the Province of Newfoundland and Labrador<br>• Department of Transportation of the Northwest Territories<br>• Department of Community Government and Transportation of the Territory of Nunavut |

[17] It is prohibited to use health cards from Manitoba, Ontario, Nova Scotia, or Prince Edward Island for the purpose of verifying identity. A health card from Quebec can be accepted if offered by the individual, but it cannot be requested.

The Company may accept a foreign ID if it is equivalent to an acceptable Canadian ID. If the ID is not in English or French, it must be translated, and the details recorded in English or French.

When verifying the identity of an individual in person, the individual's ID is examined to ensure:

- it is current (not expired);
- it is authentic, as it contains the appropriate security features or markers, and there is no evidence of tampering; and
- the picture on the ID matches the likeness of the individual whose identity is being authenticated.

When verifying the identity of individuals remotely, the Company relies on a third-party provider that verifies the authenticity of the ID, conducts "liveness testing," and confirms that the ID belongs to the individual whose identity is being verified.

The information that is recorded includes:

- the individual's name;
- the type of ID that was referenced (e.g., passport);
- the unique identifying number of the document;
- the issuing jurisdiction and country of the document;
- the expiry date (if it appears on the ID, it must be recorded); and
- the date that the document was referenced to verify the individual's identity.

### 9.3.3 VERIFYING THE IDENTITY OF AN ENTITY (8.3.3)

When verifying the identity of an entity, Brink's collects records to support the information provided about the entity and obtains and takes reasonable measures to confirm beneficial ownership, as outlined in the following section.

Brink's compares the name, address, and in the case of a corporation, the names of the directors of the entity, to supporting documents, such as those listed in the following table:

| Corporations | Entities other than a corporation |
|---|---|
| • The corporation's articles of incorporation<br>• The most recent version of a record that has to be filed annually under provincial securities legislation<br>• The most recent version of a record that confirms the corporation's existence, as well as the names of its directors | • A partnership agreement<br>• Articles of association<br>• The most recent version of a record that confirms the entity's existence, as well as its name and address |

The documents referred to must be authentic, valid, and current. The Company may rely on an electronic record, where the information is contained in a publicly available database, such as the Corporations Canada database or Canada's Business Registries, or obtain a paper record. Where a paper record is received electronically (i.e., email, fax, or scan), Brink's reviews the date of the document, as well as other features of the document for authenticity.

It is not acceptable to use verbal information to confirm an entity's identity.

If the record is in a paper format, a copy of the record must be kept. If an electronic record is referenced, the Company must retain a record that includes:

- the entity's registration number;
- the type of record consulted; and
- the source of the electronic version of the record.

## A. BENEFICIAL OWNERSHIP

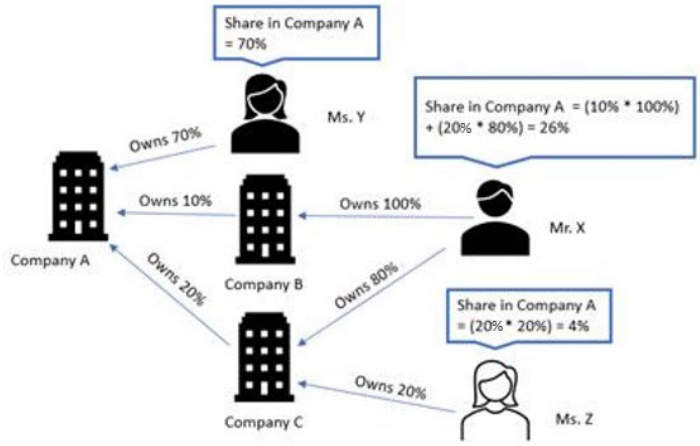
A beneficial owner is a "natural person" that directly or indirectly owns or controls 25% or more of a corporation or an entity other than a corporation, such as a partnership, or is the trustee, or known beneficiary or settlor of a trust. For entities with no ownership rights, such as a not-for-profit ("NFP"), control over the organization is solely used to establish beneficial ownership.

In addition to obtaining the beneficial ownership information about an entity, the Company must also take reasonable measures to confirm the accuracy of that information, and maintain the documents or references used to confirm the beneficial ownership structure of the entity customer in the entity customer's file.

When determining an entity's beneficial ownership, the Company searches through as many levels of information as necessary to identify all natural persons that own at least 25% of the entity and takes reasonable measures to confirm the accuracy of that beneficial ownership information.

If the Company is unable to obtain, or if after taking reasonable measures the Company is unable to confirm the accuracy of the beneficial ownership information, the Company treats the entity as high risk, and takes reasonable measures to verify the identity of the CEO or equivalent, using the identification methods described in Section 9.3.

The concept of beneficial ownership is illustrated in the following figure:




At a minimum, the Company obtains the following information:

| | |
|---|---|
| **Corporations** | • The names of all directors of the corporation; and |

| | |
|---|---|
| | • The names and addresses of all individuals who directly or indirectly own or control 25% or more of the shares of the corporation, including through bearer share holdings. |
| **Entities other than corporations** | • The names and addresses of all individuals who directly or indirectly own or control 25% or more of the entity. |
| **Trusts** | • The names and addresses of all trustees and all known beneficiaries and settlors of the trust. |
| **Widely held or publicly traded trusts** | • The names of all trustees of the trust and the names and addresses of all persons who directly or indirectly own or control 25% or more of the units of the trust. |

Applicable measures to obtain the beneficial ownership information could include inquiry, searching a public database, or reviewing documents provided by the entity customer or those obtained externally. Brink's keeps a record of the beneficial ownership information obtained as well as the measures taken to confirm the accuracy of the beneficial ownership information obtained.

In situations where there is no individual who owns or controls 25% or more of an entity, the Company similarly, keeps a record of the measures taken and the information obtained to reach this conclusion.

When determining the beneficial ownership information of an NFP, Brink's also determines whether that entity is a registered charity for income tax purposes and keeps a record to that effect. To make this determination, the Company could ask the customer questions about their charitable status, or their charitable status can be verified by consulting the charities listing on the Canada Revenue Agency website and downloading a copy of the *Directors and Trustees Worksheet* from the Registered Charity Information Return. If the entity is not a registered charity, Brink's determines whether it solicits charitable financial donations from the public and keeps a record to that effect.

As a policy, the Company does not provide services to unincorporated NFPs that are not registered with the Canada Revenue Agency as either charities or NFPs, regardless of whether or not they solicit donations from the public.

The method used to obtain beneficial ownership information must be different from the method used to confirm the beneficial ownership information. It is also acceptable to have a customer sign a document to confirm the accuracy of the beneficial ownership information obtained, which includes information on ownership, control, and structure. In this case, it is possible for one document to be used to satisfy the two steps, namely, to obtain the information and to confirm its accuracy by means of the signature.

As a policy, the Company primarily obtains and confirms beneficial ownership information by having the customer sign an attestation to confirm the veracity of the beneficial ownership information that has been provided.

For customers that are determined to be high risk as a result of having an overly complex ownership structure, or at the discretion of the Compliance Officer, Brink's may ask the customer to provide documentation that confirms beneficial ownership, such as:

- minute book;

- securities register;
- shareholders register;
- articles of incorporation;
- annual returns;
- certificate of corporate status;
- shareholder agreements;
- deed of trust;
- partnership agreements; or
- board of directors' minutes or records establishing ownership or control.

## 9.4 THIRD-PARTY DETERMINATION

Brink's takes reasonable measures to determine whether a customer is acting on behalf of a third party:

- When Brink's receives $10,000 or more in cash for transport, unless the Company is exempt from filing an LCTR (see Section 12.5) or keeping records (see Section 14) in respect of that transaction; and
- upon entering into a Service Agreement.

A third-party transaction relates to a person or entity who instructs another person or entity to conduct an activity or financial transaction on their behalf. It is not about who owns or benefits from the money, or who is carrying out the transaction or activity, but rather about who gives the instructions.

Therefore, every entity is a third party to each transaction that is conducted on its behalf, unless the person conducting the transaction is an owner or director of the entity, or an authorized employee previously documented in the Service Agreement.

When required to make a third-party determination, Brink's makes an enquiry as to whether the customer is acting on behalf of a third party, and the Company keeps a record of the customer's response. If a third-party relationship is identified, a record is retained that includes:

- the name of the third party;
- the address of the third party;
- the relationship between Brink's customer and the third party;
- the occupation/nature of business of the third party;
- the phone number of the third party, unless the third-party determination is made as a result of an LCT or large virtual currency transaction;
- the date of birth of the third party (if the third party is an individual); and
- the incorporation/registration number and jurisdiction of incorporation/registration (if the third party is an entity).

If Brink's suspects that there is a third party, but is unable to make a third-party determination, a record must be kept that includes whether the customer indicated that they were acting on behalf of a third party, and the reason that the Company suspects the involvement of a third party.

As a policy, when a third-party relationship is identified, the Company tries to onboard the third party to become a direct customer of Brink's.

An example of the Third-Party Determination Form that can be used to record details regarding third parties can be found in Appendix C.

## 9.5 BUSINESS RELATIONSHIPS

A business relationship is established when a customer conducts two or more transactions that occur within a maximum of five years from one another where the Legislation requires Brink's to verify a customer's identity as described in Section 9.3. The business relationship is established even if the Company elects not to verify the individual's identity because the identity had been previously verified or, in the case of a suspicious transaction, there is a concern that verifying the identity would alert the individual that the Company intends to submit a report to FINTRAC.

The business relationship persists for five years from the date that the customer conducted their most recent transaction.

By policy, all entity customers that have entered into a Service Agreement with Brink's are deemed to be in a business relationship.

When a business relationship is established, a record of the purpose and intended nature ("PIN") of the business relationship must be added to the customer profile. All business relationships are also subject to ongoing monitoring to:

- classify and periodically reassess customer risk level based on transactions and activities;
- keep customer identification and PIN records up to date; and
- detect any transactions that need to be reported as suspicious.

Within 30 days of the onset of a business relationship and periodically thereafter, the Company is also required to determine if an individual is a PEP/HIO. See Section 9.6.2 for more information about PEPs and HIOs.

### 9.5.1 EXCEPTIONS TO BUSINESS RELATIONSHIPS

The obligations related to business relationship requirements do not apply when the Company enters into a Service Agreement only in respect of the transportation of coins of the currency of Canada that are produced or supplied by the Royal Canadian Mint that are delivered to the Minister of Canada (or to a person designated by the Minister of Finance).

The obligations related to business relationship requirements do not apply when the Company enters into a Service Agreement only in respect of the transportation of cash, money orders, traveller's cheques, or other similar negotiable instruments between:

- the Bank of Canada and a person or entity in Canada;
- two financial entities; or
- two places of business of the same reporting entity, other than a request made by another person or entity.

### 9.5.2 PURPOSE AND INTENDED NATURE RECORD

When a business relationship is established, a record of the PIN is made. The PIN describes the nature of the business dealings with the customer and provides context for the types of transactions and activities that the customer conducts.

Examples of a PIN could include, but are not limited to:

- cash transportation from one customer location to another;
- cash transportation between a customer and another entity for business purposes;
- Fiat cash pick-up for business purposes; and/or
- BATM cash pick-up for business purposes.

### 9.5.3 CLASSIFICATION OF CUSTOMER RISK

At the onset of a business relationship, Brink's conducts and documents a risk assessment of the relationship with the customer and conducts due diligence measures consistent with Brink's Risk Assessment to ensure that enhanced measures are put in place for high-risk relationships.

Brink's assigns a risk rating to each customer. Risk ratings are applied in a manner that is consistent with Brink's Risk Assessment. A classification of high risk is determined by several factors including transaction type, certain patterns of transaction activity, and customer-specific characteristics. Customers are assessed as low risk if they are not assessed as high risk.

All information collected as part of the customer risk assessment, including if a customer is rated high risk, becomes part of the customer profile.

Excessive risk occurs in situations where the risk of dealing with a certain individual or customer type is too high for Brink's to accept their business. Brink's is prohibited from dealing with customers in these situations. Any exception to these prohibitions must be reviewed and approved by the Compliance Officer.

High-risk relationships are subject to enhanced measures put in place by the Compliance Officer to mitigate relationship-based risk. Refer to the Risk Assessment for more information about how Brink's conducts its customer risk assessment as well as the specific enhanced measures.

A customer is automatically deemed high risk if:

- the Company is unable to obtain or confirm beneficial ownership information;
- a TPR is submitted to FINTRAC (see Section 12.2);
- as a result of determining that a customer is a PEP/HIO (see Section 9.6.2); or
- if any other single high-risk factors as described in the Risk Assessment have been identified.

### 9.5.4 RECLASSIFICATION OF CUSTOMER RISK

Risk ratings are updated on an ongoing and periodic basis and are based on factors that include, but are not limited to:

- transaction activity; and
- characteristics, including PEP/HIO and sanctions status.

A reassessment of customer risk may also be triggered by:

- becoming aware of illegal or illicit activities;
- a change in characteristics, including PIN or other risk factors included in Brink's methodology for assessing customer risk;
- unexpected spikes in customer activity; and
- submitting a report to intelligence, regulatory, or law enforcement agencies with respect to suspicious transactions or terrorist property.

At a minimum, the Company reviews the customer risk according to the customer information update schedule that is specified in Section 9.5.5 and, if necessary, conducts a reassessment of the customer's risk, based on the outcome of the review.

Refer to the Risk Assessment for more information on how Brink's conducts its customer risk assessments.

### 9.5.5 KEEPING CUSTOMER INFORMATION UP TO DATE

For all customers classified as being in a business relationship, the Company periodically reviews customer information to ensure that the information contained in the Company's records is up to date.

The minimum frequency with which this information is updated is based on the ML/TF risk level associated with each customer.

High-risk customer information is reviewed at least annually, and low-risk customer information is reviewed at least every three years.

Customer information is updated on an ongoing basis, if in the course of operations new information becomes available. If during a customer information review, any of the following has not been updated, Brink's takes steps to update the following information:

- Customer name;
- Customer address;
- Customer occupation/nature of principal business (see Section 14.2);
- Customer telephone number and email;
- Customer PEP/HIO status; and
- List of authorized employees conducting transactions on behalf of an entity customer.

The PIN record is considered during reviews of unusual transactions and during scheduled transaction reviews. If the transaction activity does not appear to be consistent with the stated PIN, the customer is contacted to update it.

Brink's also reviews to determine if there have been changes to the entity's beneficial ownership structure and/or its directors. If Brink's identifies a change to the beneficial ownership structure, the Company must take reasonable measures to confirm the new beneficial ownership information, as well as the actions described in Section 9.3.3(A) if those measures are unsuccessful.

### 9.5.6 ONGOING MONITORING OF TRANSACTIONS

Brink's monitors the transactions of its business relationships for evidence of certain patterns of activity that could be indicative of suspicious activity, such as whether the transactions are consistent with the information known about the customer or the transactions are demonstrative of known suspicious indicators. Monitoring is also conducted

to determine whether a customer's current risk rating needs to be adjusted, and to meet Brink's reporting requirements as set out in Section 12.

Transaction monitoring is conducted systematically by Brink's third-party systems both in real-time and historically by generating alerts for transactions and transaction patterns that meet a series of rules within the system. The rules are maintained by the Compliance Officer separately from this document. These rules are based on a variety of attributes and related formulas that are associated with higher ML/TF risk in publications issued by FINTRAC and the FATF and adjusted for based on the Company's Risk Assessment. Alerts can be triggered by events such as:

- Complex or unusual transactions;
- Transaction activity inconsistent with customer behaviour;
- Transaction volumes in excess of expectations;
- Transactions from and/or to high-risk jurisdictions; and/or
- Any other activity which the Company regards as particularly likely by its nature to be related to ML/TF.

System generated alerts are manually reviewed by compliance analysts to further assess whether the transaction represents unusual activity, whether an adjustment to the customer's risk rating or behaviour settings is required, whether a customer interview is necessary, or if there is sufficient knowledge about the customer and the related transaction to close the alert. If any indicators of ML/TF are detected, it is escalated by the Compliance Team to the Compliance Officer for further review and investigation via the Company's internal Ethics hotline at +1-877-275-4585 (https://Brinkshotline.ethicspoint.com) or Brink's Compliance team's email address (BrinksCanadaKYC@brinks.com). In all cases, the resolution and/or escalation of the alert is documented in the system.

For each customer that is determined to be high risk, on a quarterly basis, the Compliance Officer conducts a manual review of all transactions conducted by the customer during the previous period. The purpose of the review is to examine a larger sample of transactions and changes in behaviour or characteristics over time to identify previously undetected and potentially suspicious activity and conduct an investigation as set out in Section 12.3.

A record of the ongoing transaction monitoring conducted is maintained as outlined in Section 14.

## 9.6 CUSTOMER SCREENING

The following section lays out the policies and procedures with respect to customer screening.

### 9.6.1 POTENTIAL SANCTIONS MATCHES

Brink's does not knowingly enter into transactions with, or provide or assist transfers to, or for the benefit of, governments, entities, charities, organizations, and individuals targeted by required sanctions, including, but not limited to, Canadian anti-terrorism measures and Canadian economic sanctions. To that end, Brink's screens its customer database and payments records for the names of Designated Persons.

Brink's scans the full name of entity customers and their Principals at onboarding and periodically thereafter (as described in Section 9.5.5) to find potential name matches.

Ongoing scans are also conducted based on watchlist updates, changes to the customer's risk profile, or changes to customer information. Beneficiaries are screened at the time of the transaction.

At a minimum, Brink's screens against the prevailing lists promulgated pursuant to the following laws:

- Criminal Code;
- United Nations Act;
- Sergei Magnitsky Law;
- Freezing the Assets of Corrupt Foreign Officials Act; and
- SEMA.

In addition, screening is conducted against the prevailing versions of lists maintained by the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC"), and include:

- Specially Designated Nationals ("SDN") list; and
- OFAC Consolidated Sanctions list.

To adjudicate a potential name match, common differentiators such as date of birth or country of origin are compared to identification information collected to determine the veracity of the match.

If the match is a true match, any customer funds in possession are held and no transactions are processed (regardless of the status of the transactions) without an evidence-based discount of the match, or written judicial, law enforcement, or ministerial direction.

Where required by Legislation, the Compliance Officer reports to the required entities in the prescribed format, within the legislated timeline (see Section 12.2).

### 9.6.2 POLITICALLY EXPOSED PERSONS DETERMINATION

The Legislation seeks to control corruption by increased scrutiny of activity involving people who hold, or who have held positions of public trust, which provide influence that might be exploited for personal gain. To this end, it imposes required measures for certain categories of individuals, collectively referred to in this document as PEPs.

A full list of PEPs as defined by Legislation are listed in Appendix D, but can be summarized into the following categories:

a) PEFP: Politically Exposed Foreign Person (those who hold, or have ever held, such a position);
b) PEDP: Politically Exposed Domestic Person (those who hold, or have held, such a position in the preceding five years);
c) HIO: Head of an International Organization (those who hold, or have held, such a position in the preceding five years); and
d) A family member or close associate of a PEFP, PEDP, or HIO.

Brink's takes reasonable measures to determine PEP status:

- within 30 days of a business relationship being established and periodically thereafter, according to the frequency described in Section 9.5.5;

- within 30 days of detecting a fact that a customer in a business relationship may be a PEP, which could include, but is not limited to, documenting occupation, updating customer information, or as a result of a negative news search;
- within 30 days of a request by a person[18] to transport cash equivalent to $100,000 or more;
- within 30 days of a request by a person[19] to transport money orders, traveller's cheques, or other similar negotiable instruments equivalent to $100,000 or more; and/or
- within 30 days of a request by a person[20] to transport cash in an amount that is not declared or cannot be readily determined.

Unless a person has already been determined to be a PEP, a PEP determination must be made upon a triggering event regardless of whether a PEP determination has been previously conducted.

If information with respect to third parties or counterparties is also collected as part of any of the above triggers, Brink's also makes a PEP determination on those parties.

Reasonable measures to make a PEP determination include:

- asking the customer if they are a PEP and documenting their response; and/or
- independently confirming the customer's PEP status by using an industry-recognized database.

Brink's uses an external industry-recognized software provider to conduct PEP determinations on individual customers and the Principals of entity customers at onboarding as well as during triggering activities as described above.

Upon determining that a person is a PEP, Brink's takes the measures described in the following table, within 30 days of the date on which the PEP determination triggered occurred:

| Enhanced measures<br>PEP determination trigger | Reasonable measures to determine the customer's source of wealth | Reasonable measures to determine source of funds that was used for the transaction | Senior Management review |
|---|---|---|---|
| **Entering into a business relationship or during a periodic review/when a fact is detected** | Yes | --- | --- |
| **Transporting $100,000 or more in cash** | Yes | Yes | Yes |
| **Transporting cash in an amount that is not declared or cannot be readily determined[21]** | Yes | Yes | Yes |

[18] The requirements for PEP determinations apply when the request is received from a "person" who is defined as an "individual" in the PCMLTFA.
[19] See previous footnote.
[20] See previous footnote.
[21] The requirements for PEP determinations apply when the request is received from a "person" who is defined as an "individual" in the PCMLTFA.

| | | | |
|---|---|---|---|
| **Transporting $100,000 or more in money orders, traveller's cheques, or other similar negotiable instruments** | Yes | Yes | Yes |

Reasonable measures to obtain source of wealth or source of funds include asking the customer or requesting a copy of supporting documents, which include but are not limited to a bank statement or letter of employment for source of wealth or pay stub or bill of sale for source of funds.

If an individual customer or the Principal of an entity customer is determined to be a PEP, the Company considers the individual customer or the entity to be high risk for the duration of their relationship with the Company, subject to the Company's enhanced measures for high-risk customers.

In addition, the following records are maintained with respect to PEPs:

- the office or position of the PEP;
- the name of the organization or institution of the PEP;
- the date that Brink's made the determination that the individual is a PEP;
- where it is determined that an individual is a prescribed relative or close associate of a PEP, the relationship between the individual and the PEP;
- the source of the individual's wealth, if obtained (as required see table above);
- the source of the funds that were used for the transaction, if obtained (as required, see table above);
- the name of the member of Senior Management who reviewed the transaction and the date of the review (as required, see table above).

Brink's records the above information in the customer profile. A sample PEP Approval Form can be found in Appendix E.

### A. EXCEPTIONS TO POLITICALLY EXPOSED PERSONS DETERMINATIONS

Brink's is not required to take reasonable measures to conduct a PEP determination in respect of the transportation of coins of the currency of Canada that are produced or supplied by the Royal Canadian Mint that are delivered to the Minister of Canada (or to a person designated by the Minister of Finance).

Brink's is not required to take reasonable measures to conduct a PEP determination in respect to the transportation of cash, money orders, traveller's cheques, or other similar negotiable instruments is between:

- the Bank of Canada and a person or entity in Canada;
- two financial entities; or
- two places of business of the same reporting entity, at their request.

## 10. Ministerial Directives

Under Part 1.1 of the PCMLTFA, which came into force on June 19, 2014, the Minister of Finance may:

- issue directives that require reporting entities to apply countermeasures to transactions coming from or going to designated foreign jurisdictions or entities; and
- recommend the introduction of regulations to restrict reporting entities from entering a financial transaction coming from or going to designated foreign jurisdictions or entities.

These authorities allow the Minister of Finance to take steps to protect Canada's financial system from foreign jurisdictions and foreign entities that are considered to present high risks for facilitating ML/TF.

## 10.1 HOW BRINK'S BECOMES AWARE OF MINISTERIAL DIRECTIVES

While directives are issued by the Minister of Finance, FINTRAC informs reporting entities that a directive has been issued by publishing it to its website. Each directive includes an outline of countermeasures that are limited to the same activities for which reporting entities already have obligations. The countermeasures enhance or add to these obligations.

- Directives specify the date they come into force and remain in force until officially revoked, suspended, or amended.
- Directives are reviewed by the Minister of Finance at least every three years from the day they take effect.

The Compliance Officer reviews the FINTRAC website periodically to ensure Brink's becomes aware of Ministerial Directives that are currently in force.

## 10.2 RESPONDING TO MINISTERIAL DIRECTIVES

When Brink's becomes aware of a ministerial directive, the Compliance Officer:

- reviews the directive;
- determines the impact of the directive on the Company's Risk Assessment; and
- where the Ministerial Directive impacts operations, updates the Program, and ensures the implementation of the countermeasures specified in the directive.

## 10.3 MINISTERIAL DIRECTIVES IN FORCE

### 10.3.1 DECEMBER 9, 2017: DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA

The Minister of Finance issued this directive in response to a public statement from the FATF on November 3, 2017, in which the FATF expressed its particular and exceptional concerns about North Korea's failure to address the significant deficiencies in its AML/CTF regime and the serious threat this poses to the integrity of the international financial system.

This Ministerial directive requires that all transactions to and from North Korea be treated as high risk, regardless of the amounts of the transactions.

The Company monitors for the following key indicators to assess involvement of its customer in transactions to or from North Korea:

- Explicit direct involvement in the country;
- Involvement with neighbouring countries;
- Involvement of North Korean Won;

- Connection with individuals or entities with substantial financial ties to North Korea; and/or
- Documented ties, represented ties, or inferred ties to North Korea based on facts, context, and indicators.

Brink's has determined that conducting transactions involving the transfer of funds to and/or from North Korea is outside of its risk tolerance and is, therefore, restricted.

### 10.3.2 JULY 25, 2020: ISLAMIC REPUBLIC OF IRAN

The Minister of Finance issued this directive in response to a public statement issued by the FATF in February 2020, in which the FATF expressed its particular and exceptional concerns regarding Iran's failure to address the significant deficiencies in its AML/CTF regime and the serious threat this poses to the integrity of the international financial system. This directive requires that Reporting Entities:

- treat every financial transaction originating from or bound for Iran, regardless of its amount, as a high-risk transaction;
- verify the identity of any customer (person or entity) requesting or benefiting from such a transaction;
- exercise EDD, including ascertaining the source of funds in any such transaction, the purpose of the transaction and, where appropriate, the beneficial ownership or control of any entity requesting or benefiting from the transaction;
- keep and retain a record of any such transaction; and
- report all such transactions as set out in Section 12.3.

Brink's does not accept or provide payment in Iranian Rial nor send or receive payments to or from Iran. Consequently, this directive is not deemed to have an effect on the Company's operations.

The Company also monitors for the following key indicators to assess involvement of its customers in transactions to or from Iran:

- Explicit direct involvement in the country;
- Involvement with neighbouring countries;
- Involvement of Iranian Rial;
- Connection with individuals or entities with substantial financial ties to Iran; and/or
- Documented ties, represented ties, or inferred ties to Iran based on facts, context, and indicators.

If an indicator is discovered, Brink's adds the customer's personal information to a blacklist to ensure they cannot conduct further transactions. The Company takes the appropriate actions related to any transaction that may have been completed.

### 10.3.3 FEBRUARY 24, 2024: RUSSIA

Canada's Minister of Finance issued this directive based on the determination that Russia's national AML/CTF measures are both insufficient and ineffective, as well as the risk that Russia may be facilitating the financing of threats to Canada's security, which could have an adverse impact on the integrity of the Canadian financial system or the reputational risk to that system.

This directive requires that Reporting Entities:

- treat every financial transaction originating from or bound for Russia, regardless of its amount, as a high-risk transaction;
- verify the identity of any customer (person or entity) requesting or benefiting from such a transaction;
- exercise EDD in relation to any such transaction, including ascertaining the source of funds or virtual currency, the purpose of the transaction, and the beneficial ownership and control of any entity requesting or benefitting from the transaction;
- keep and retain a record of any such transaction, in accordance with the PCMLTFA and associated Regulations, regardless of its amount.

Examples of transactions that would be considered to originate from or bound to Russia include, but are not limited to:

- EFTs, remittances, or other transfers that include a Russian originating or destination address - this may include transactions where the ordering person or entity, beneficiary, or third-party details are Russian;
- the activities of representatives of the Government of Russia (for example, transactions on an Embassy of Russia's bank account in Canada);
- the activities of representatives of the Government of Russia;
- receiving Russian Rouble as a deposit to an account or for a virtual currency transaction; conducting a foreign currency or virtual currency exchange transaction that includes Russian Rouble (for example, CAD to Russian Rouble, Russian Rouble to U.S. Dollar, virtual currency to Russian Rouble, etc.); and
- issuing or redeeming bank drafts or other negotiable instruments that include a Russian Rouble component.

For clarity, *in the absence of other indicators, the fact that a customer is Russian is not sufficient to suggest that a transaction is originating from or destined for Russia.*

The Company monitors for the following key indicators to assess involvement of its customers in transactions to or from Russia:

- Explicit direct involvement in the country;
- Involvement with neighbouring countries;
- Involvement of Russian Rouble;
- Connection with individuals or entities with substantial financial ties to Russia; and/or
- Documented ties, represented ties, or inferred ties to Russia based on facts, context, and indicators.

Brink's does not accept or provide payment in Russian Rouble nor send or receive transactions to or from Russia. Consequently, this directive is not deemed to have an effect on the Company's operations.

## 11. Law Enforcement Inquiries and Requests

Any requests from law enforcement are treated in a confidential manner and forwarded to the Compliance Officer for review and appropriate response, which must include co-operation with all judicially authorized formal information requests and orders.

Upon receipt of any formal requests from law enforcement, the Compliance Officer must provide all relevant information in a timely manner. Additionally, the Compliance Officer maintains a log of such requests, including the information provided.

A law enforcement request triggers a reassessment of customer risk. Depending on the outcome of the review, Brink's may elevate the risk profile of the customer and/or monitor the customer's transaction activity and behaviour. The Company also considers whether filing an STR with FINTRAC is warranted, such as when the request is a formal production order.

In the event the risk to maintain a business relationship is found to be outside of the entity's risk tolerance, Brink's should consider divesting from the relationship.

Senior Management is notified of any inquiry or request received from law enforcement. The law enforcement inquiries and requests can include, but are not limited to, production orders and tax authority requests.

## 12. Reporting

As a Reporting Entity, Brink's has obligations to report certain prescribed transactions to FINTRAC, and other agencies, such as the Canadian Security Intelligence Service ("**CSIS**") or the RCMP, when necessary.

For the purposes of determining whether a reporting threshold has been met for a transaction conducted in a foreign currency, the equivalent value in Canadian dollars is calculated using the last rate provided by the Bank of Canada available at the time of the transaction.

The Compliance Officer is responsible for ensuring reports are submitted for all prescribed transactions within the timeframes and in the format required, as defined in the following table:

| Report Type | Timing | Reported To | Submission Method |
|---|---|---|---|
| TPR | Immediately | FINTRAC, RCMP, CSIS | On paper (via fax) |
| STR | As soon as practicable from the date that a fact is discovered that causes the Company to have reasonable grounds to suspect that the activity could be related to ML/TF | FINTRAC | Electronically via FINTRAC web reporting system |
| Sanctions Evasion STR | As soon as practicable where there are reasonable grounds to suspect sanctions evasion by someone acting on behalf of a sanctioned person | FINTRAC | Electronically via FINTRAC web reporting system |
| LCTR | 15 calendar days from the transaction date | FINTRAC | Electronically via FINTRAC web reporting system |

## 12.1 AGGREGATION OVER THE 24-HOUR RULE

Brink's is required to determine a static 24-hour window to identify transactions that need to be aggregated and reported under the 24-hour rule, specifically LCTRs. Whenever the Company is required to aggregate transactions within a 24-hour period, the Company uses a static period referred to as the Company's "24-hour period," which extends from 12:00:00 am Eastern Time ("ET") to 11:59:59 pm ET.

Each transaction that falls under the 24-hour rule within the Company's 24-hour period is viewed independently from the previous or subsequent static 24-hour window so that one transaction does not overlap multiple 24-hour windows.

Brink's continues to monitor all transactions, regardless of the static 24-hour period, to identify suspicious transactions that could relate to ML/TF as described in 12.3.

The table below provides an overview of how the 24-hour rule can be applied for LCTR transactions:

| **Transactions in a 24-hour period that total $10,000 or more** | **Aggregated in a single report** |
|---|---|
| 2 or more transactions under $10,000 | Yes |
| 1 or more transactions under $10,000 and 1 or more transactions at $10,000 or more | Yes |
| 2 or more transactions at $10,000 or more | Yes |

### 12.1.1 REPORTS WHERE ALL TRANSACTIONS ARE THE SAME

Brink's is only required to send one report to FINTRAC in the situation where two or more reports contain transactions that are all the same.

For example, Client A conducts an LCT for $8,000 and later in the day, conducts a second LCT for $6,000. Client A is both the conductor and the beneficiary.

Although two reports are required, one based on conductor and one based on beneficiary, the Company can choose to send only one report because the information is exactly the same.

Only when the transactions are all exactly the same but have different aggregation types (conductor and beneficiary for example) can Brink's choose to submit only one report based on one aggregation type.

To ensure a consistent approach to reporting, Brink's policy will be to report based on beneficiary.

### 12.1.2 REPORTS FOR SINGLE TRANSACTIONS OF $10,000 OR MORE WITHIN A 24-HOUR PERIOD

When the Company has a single transaction in the amount of $10,000 or more in a 24-hour window, it must report this transaction in its own report to FINTRAC unless it can be aggregated with any other transaction(s).However, if a transaction in the amount of $10,000 or more is being aggregated and reported with other transactions, then Brink's does not need to report this transaction in its own report.

For example, Client A conducts three transactions within a 24-hour period, one is $5,000, one is $4,000, and one is $11,000.

The Company would be required to report all three transactions in a single report. The $11,000 transaction would be included in the LCTR and, as such, would not need to be reported separately as a single transaction.

### 12.1.3 INSTANCES WHERE AGGREGATION IS NOT PERMITTED

When a person or entity has different roles (conductor/requestor, on behalf of, or beneficiary) in different transactions, the requirement to aggregate transactions is not triggered.

For example, aggregation would not be required:

- when a transaction is conducted by an entity (for example, Client X), and
- a second transaction is conducted by someone else on behalf of Client X.

This is because both transactions are not conducted by the same person or entity nor are they conducted on behalf of the same person or entity. Instead, Client X is the conductor of the first transaction and is the on behalf of party in the second transaction.

### 12.1.4 AGGREGATION EXAMPLES OF LCT TRANSACTIONS

#### A. LCTR EXAMPLE 2: RECEIPT OF CASH – 24-HOUR RULE – AGGREGATION ON THE BENEFICIARY – TRANSACTIONS OCCURRING IN DIFFERENT TIME ZONES

The 24-hour window for the LCTR process is from 12 am to 11:59 pm the same day based on EST.

- Transaction 01: Monday at 10:08 am EST, the MSB receives $7,000 cash from Customer A in Ottawa for transport to Entity B.
- Transaction 02: Monday at 11:43 am EST, the MSB receives $3,000 cash from Customer B in Montreal for transport to Entity B.
- Transaction 03: Monday at 5:10 pm Pacific Standard Time (PST), the MSB receives $2,000 cash from Customer C in Victoria for transport to Entity B.
- Transaction 04: Monday at 9:12 pm PST, the MSB receives $4,000 cash from Customer D in Victoria for transport to Entity B.

The following table summarizes the above example:

| 24-hour window | Transaction Reference Number | Time of Transaction | Amount ($) | Conductor | Beneficiary | Third party | Aggregation Type |
|---|---|---|---|---|---|---|---|
| 12 am to 11:59 pm EST (Monday) | 01 | 10:08 am EST | 7,000 | Customer A | Entity B | None | Beneficiary |
| | 02 | 11:43 am EST | 3,000 | Customer B | Entity B | None | Beneficiary |
| | 03 | 5:10 pm Pacific | 2,000 | Customer C | Entity B | None | Beneficiary |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | Standard Time (PST), Monday (which equals to 8:10 pm EST, Monday) | | | | | |
| 12 am to 11:59 pm EST (Tuesday) | 04 | 9:12 pm PST, Monday (which equals to 12:12 am EST, Tuesday) | 4,000 | Customer D | Entity B | None | Not applicable |

**LCTR requirement**

In this scenario, the MSB has locations that are in 2 different time zones:

- EST (Ottawa and Montreal)
- PST (Victoria)

Because the MSB's time zone for its 24-hour window is based on EST, it must convert the time of any transaction that occurs in PST to EST to confirm if it falls within its 24-hour window. The MSB would then review all transactions that fall within the 24-hour window to check if multiple transactions occurred for the same aggregation type that together total $10,000 or more. The MSB would notice:

- Transactions 01, 02 and 03 all have Entity B as the beneficiary and total $12,000 and occur in the same 24-hour window even though they all are conducted at locations with different time zones.
- Transaction 04 for $4,000 also has Entity B as the beneficiary but it does not occur in the same 24-hour window as transactions 01, 02 and 03.

The MSB submits 1 report:

- Report 1: An LCTR under the 24-hour rule that includes 3 transactions (01, 02 and 03) totalling an amount equivalent to $12,000 aggregated on the beneficiary, which is Entity B. Although Entity B is also the beneficiary of transaction 04, it is not aggregated with transactions 01, 02 and 03 because it was conducted on Monday at 9:12 pm PST (which equals to 12:12 am EST, Tuesday) and therefore falls in the next 24-hour window.

### B. LCTR EXAMPLE 3: RECEIPT OF CASH – 24-HOUR RULE – AGGREGATION ON THIRD PARTY

The 24-hour window for the LCTR process is from 12 am to 11:59 pm the same day.

- Transaction 01: Friday at 11:12 am, the MSB receives $12,000 cash from Customer A for transport to James. The MSB knows that Customer A conducted the transaction on behalf of Client A.
- Transaction 02: Friday at 1:32 pm, the MSB receives $4,000 cash from Customer B for transport to Customer A. The MSB knows that Customer B conducted the transaction on behalf of Customer A.

The following table summarizes the above example:

| 24-hour window | Transaction Reference Number | Time of Transaction | Amount ($) | Conductor | Beneficiary | Third party | Aggregation Type |
|---|---|---|---|---|---|---|---|
| 12 am to 11:59 pm | 01 | 11:12 am | 12,000 | Customer A | Customer B | Customer A | Third party |
| | 02 | 1:32 pm | 4,000 | Customer B | Customer A | Customer A | Third party |

**LCTR requirement**

In this scenario, the MSB would review all transactions that fall within the 24-hour window to check if multiple transactions occurred for the same aggregation type that together total $10,000 or more. The MSB would notice:

- Transactions 01 and 02 were both conducted on behalf of Customer A (third party) and total $16,000.

The MSB submits 1 report:

- Report 1: An LCTR under the 24-hour rule that includes two transactions (01 and 02) totalling an amount equivalent to $16,000 aggregated on the third party, which is Customer A.

Transaction 01 (in the amount of $12,000) is over $10,000 but does not need to be reported in its own report, as this transaction has been included in report 1 that is aggregated by third party.

A transaction in the amount of $10,000 or more must be reported in its own report if the transaction has not been aggregated with other transactions in a 24-hour window.

### C. LCTR EXAMPLE 4: RECEIPT OF CASH – 24-HOUR RULE – AGGREGATION ON CONDUCTOR – ENTITY OR PERSON

The 24-hour window for the LCTR process is from 12 am to 11:59 pm the same day.

- Transaction 01: Wednesday at 1:30 pm, the MSB receives $5,000 cash from Yara who is the President of The Rosie Kitchen Supply Company for transport. The MSB asks Yara if

she is conducting this transaction in her capacity as the President of The Rosie Kitchen Supply Company. Yara confirms that she is acting in her capacity as the President of The Rosie Kitchen Supply Company for this transaction. Yara is therefore understood to be acting as the entity (Rosie Kitchen Supply Company).

- Transaction 02: Wednesday at 1:40 pm, the MSB receives $6,000 cash from Yara for transportation. Golden Bank asks Yara if she is conducting this transaction in her capacity as the President of The Rosie Kitchen Supply Company. Yara advises that she is not conducting this transaction in her capacity as the President of The Rosie Kitchen Supply Company as the transport of cash is for her personal reasons. Yara is therefore understood to be acting as a person.
- Transaction 03: Wednesday at 3:05 pm, the MSB receives $8,000 cash from Yara who requests a cash transportation. the MSB asks Yara if she is conducting this transaction in her capacity as the President of The Rosie Kitchen Supply Company. Yara advises that she is conducting this transaction in her capacity as the President of The Rosie Kitchen Supply Company. Yara is therefore understood to be acting as the entity (Rosie Kitchen Supply Company).

The following table summarizes the above example:

| 24-hour window | Transaction Reference Number | Time of Transaction | Disposition Type | Amount ($) | Conductor | Beneficiary | Third party | Aggregation Type |
|---|---|---|---|---|---|---|---|---|
| 12 am to 11:59 pm | 01 | 1:30 pm | Cash transportation | 5,000 | The Rosie Kitchen Supply Company | The Rosie Kitchen Supply Company | None | Conductor |
| | 02 | 1:40 pm | Cash transportation | 6,000 | Yara | Yara | None | Not applicable |
| | 03 | 3:05 pm | Cash transportation | 8,000 | The Rosie Kitchen Supply Company | The Blueberry Company | None | Conductor |

**LCTR requirement**

1. Business Practice to Treat an Entity as the Conductor

   In this scenario, the MSB has a business practice (which is explained in its policies and procedures) to treat an entity as the conductor when the President (or CEO) of an entity conducts a transaction and the MSB is aware that the individual is acting as the entity in their capacity as the President. This business practice is in line with FINTRAC's policy interpretation that an entity can only conduct a transaction by means of a physical person, and when that person is the President, CEO, or someone who holds an equivalent position within the entity, they can be considered to be acting as the entity. The MSB would review

all transactions that fall within the 24-hour window to check if multiple transactions occurred for the same aggregation type that together total $10,000 or more. It would notice:

- Transactions 01 and 03 were both conducted by The Rosie Kitchen Supply Company and total $13,000.

The MSB submits 1 report:

- Report 1: An LCTR under the 24-hour rule that includes 2 transactions (01 and 03) totalling an amount equivalent to $13,000 aggregated on the conductor, which is The Rosie Kitchen Supply Company.

2. Business practice to treat a person (individual) as the conductor

If the MSB has instead a business practice (which is explained in its policies and procedures) to treat a person (individual) as the conductor, regardless of the person's role, then the MSB would notice that transactions 01, 02 and 03 were all conducted by Yara and total $19,000. The MSB would also notice that transactions 01 and 03 were conducted by Yara on behalf of The Rosie Kitchen Supply Company and total $13,000.

The following table summarizes #2:

| 24-hour window | Transaction Reference Number | Time of Transaction | Disposition Type | Amount ($) | Conductor | Beneficiary | Third party | Aggregation Type |
|---|---|---|---|---|---|---|---|---|
| 12 am to 11:59 pm | 01 | 1:30 pm | Cash transportation | 5,000 | Yara | The Rosie Kitchen Supply Company | The Rosie Kitchen Supply Company | Conductor |
| | 02 | 1:40 pm | Cash transportation | 6,000 | Yara | Yara | None | Conductor |
| | 03 | 3:05 pm | Cash transportation | 8,000 | Yara | The Blueberry Company | The Rosie Kitchen Supply Company | Conductor |

The MSB submits 2 reports:

- Report 1: An LCTR under the 24-hour rule that includes 3 transactions (01, 02 and 03) totalling an amount equivalent to $19,000 aggregated on the conductor, which is Yara.
- Report 2: An LCTR under the 24-hour rule that includes 2 transactions (01 and 03) totalling an amount equivalent to $13,000 aggregated on the **third party**, which is The Rosie Kitchen Supply Company.

These 2 reports contain some transactions that are the same (transactions 01 and 03), but some that are different. The first report aggregated by conductor contains 1 additional transaction (transaction 02) that is not in the second report aggregated by third party.

To ensure a consistent approach to reporting, Brink's policy will be to treat an entity as the conductor when the President (or CEO) of an entity conducts a transaction and the MSB is aware that the individual is acting as the entity in their capacity as the President.

## 12.2 TERRORIST PROPERTY REPORTS

A TPR is submitted to FINTRAC if the Company is required to make a disclosure under subsection 83.1(1) of the Criminal Code, SEMA, the Sergei Magnitsky Law, or the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism ("RIUNRST"), with respect to property owned or controlled by a terrorist group or a listed individual or entity.

TPRs differ from other reporting types, in that it is the existence of property, and not necessarily a transaction or attempted transaction, that triggers the reporting requirement.

Property is anything owned or controlled by an individual or entity, whether tangible or intangible. It includes real and personal property, as well as deeds or instruments giving title or right to property or giving right to receive money or goods. It also includes any property that has been converted or exchanged or acquired from any conversion or exchange.

Examples of property include:

- cash;
- virtual currency;
- monetary instruments (e.g., cheques, bank drafts, money orders);
- bank accounts (including registered savings accounts);
- prepaid payment products or accounts;
- casino or gaming products and tokens;
- securities (such as stocks, bonds, mutual funds);
- jewelry or precious metals or stones;
- real estate (including any instrument that gives right to real estate property, such as a deed); or
- insurance policies.

Scanning for the names of terrorist groups, or listed individuals or entities is conducted as part of Brink's screening for potential sanctions matches, as described in Section 9.6.1. Brink's may also come across publicly available information in the normal course of operations that may be indicative of potential terrorist property. Potential terrorist property is escalated to the Compliance Officer for investigation immediately.

Regardless of the status of the transactions, no transactions are processed, including the return of property, without an evidence-based discount of the match, or written judicial, law enforcement, or ministerial direction.

If it is known that a transaction is related to property owned or controlled by or on behalf of a terrorist group or believed that the property is owned or controlled by or on behalf of a listed person, the transaction must not be completed. This property must be frozen as per the Criminal Code and the RUINRST.

If a transaction or attempted transaction involves property for which a TPR has been filed, an STR must also be submitted to FINTRAC, as described in Section 12.3. An STR is also filed, if it is suspected that a transaction or attempted transaction involves property owned or controlled by a terrorist, terrorist group or a listed individual or entity (i.e., even if the threshold for a TPR has not been met).

### 12.2.1 DISCLOSURES REQUIRED UNDER THE CRIMINAL CODE

Under subsection 83.1(1) of the Criminal Code, Brink's is required to disclose, without delay, to the Commissioner of the RCMP or to the Director of CSIS the existence of property in its possession or control that is known to be owned or controlled by or on behalf of a terrorist group. In addition, the Company must disclose, to the RCMP or CSIS, information about any transaction or proposed transaction in respect of that property.

A terrorist group is defined as:

- an entity that has as one of its purposes or activities facilitating or carrying out any terrorist activity;
- a listed entity; or
- an association of such entities.

An entity for these purposes could include a person, group, trust, partnership or fund, or an unincorporated association or organization. A listed entity is one that appears on a list established by section 83.05 of the criminal code, which has identified entities as being associated with terrorist activity. A terrorist group also includes groups included on official, publicly available lists relating to terrorist activity (e.g., OFAC lists).

### 12.2.2 DISCLOSURES UNDER THE UNITED NATIONS RESOLUTIONS ON THE SUPPRESSION OF TERRORISM

Under subsection 8(1) of RIUNRST, Brink's is required to disclose, without delay, to the Commissioner of the RCMP or to the Director of CSIS the existence of property in its possession or control that the Company has reason to believe is owned, held, or controlled by or on behalf of a listed person. In addition, the Company must disclose, to the RCMP or CSIS, information about any transaction or proposed transaction in respect of that property.

A listed person is an individual or entity that is listed in the Schedule of the RIUNRST because there are reasonable grounds to believe that the individual or entity:

- has carried out, attempted to carry out, participated in or facilitated the carrying out of a terrorist activity;
- is controlled directly or indirectly by any such individual or entity; or
- is acting on behalf of, or at the direction of, or in association with any such individual or entity.

### 12.2.3 DISCLOSURES UNDER THE SPECIAL ECONOMIC MEASURES ACT

The SEMA regulations require Brink's to disclose, without delay, to the Commissioner of the RCMP or to the Director of CSIS the existence of property in its possession or control that the Company has reason to believe is owned, held, or controlled by or on behalf of a listed person. In addition, the Company must disclose, to the RCMP or CSIS, information about any transaction or proposed transaction in respect of that property. A listed person is an individual or entity that is listed in the schedule of a SEMA regulation.

#### A. OWNERSHIP AND CONTROL

If it is determined that a listed individual owns or controls an entity, the property of that entity must additionally be disclosed to the RCMP or CSIS, as well as information about any transaction or proposed transaction in respect of that property.

For the purpose of SEMA, an individual is considered to own or control an entity if:

- the person holds 50% or more of an entity's shares, ownership interests or voting rights;
- the person is able to change the composition or powers of the entity's board of directors; or
- it is reasonable to conclude that the person is able to directly or indirectly direct the entity's activities.

### 12.2.4 DISCLOSURES UNDER THE SERGEI MAGNITSKY LAW

Under the Sergei Magnitsky Law, Brink's is required to disclose, without delay, to the Commissioner of the RCMP or to the Director of CSIS the existence of property in its possession or control that the Company has reason to believe is owned, held, or controlled by or on behalf of a listed person. In addition, the Company must disclose, to the RCMP or CSIS, information about any transaction or proposed transaction in respect of that property. A listed person is an individual or entity that is listed in the schedule of a regulation promulgated under the Sergei Magnitsky Law.

#### A. OWNERSHIP AND CONTROL

If it is determined that a listed individual owns or controls an entity, the property of that entity must additionally be disclosed to the RCMP or CSIS, as well as information about any transaction or proposed transaction in respect of that property.

For the purpose of the Sergei Magnitsky Law, an individual is considered to own or control an entity if:

- the person holds 50% or more of an entity's shares, ownership interests or voting rights;
- the person is able to change the composition or powers of the entity's board of directors; or
- it is reasonable to conclude that the person is able to directly or indirectly direct the entity's activities.

### 12.2.5 TPR SUBMISSION AND TIMEFRAME

TPRs must be submitted to FINTRAC immediately.

Unlike other types of reports that are submitted to FINTRAC electronically, TPRs must be completed using a paper form[22] and submitted to FINTRAC by fax (1-866-226-2346), if the Company has the technical capability to do so. If the Company does not have the capability to submit the TPR by fax, the TPR must be sent by regular or registered mail to:

Financial Transactions and Reports Analysis Centre of Canada

Section A

234 Laurier Avenue West, 24th Floor

Ottawa, ON

K1P 1H7

There is no acknowledgement of receipt when a TPR is submitted. Upon submitting a TPR to FINTRAC, Brink's immediately notifies the CSIS Terrorist Financing Unit by fax at 613-369 2303, as well as the RCMP at 613-825-7030.

Refer to the FINTRAC website for details on the information that should be included in a TPR.[23]

Brink's maintains a copy of all TPRs filed with FINTRAC (see Section 14).

## 12.3 SUSPICIOUS TRANSACTIONS AND ATTEMPTED SUSPICIOUS TRANSACTIONS

An STR is submitted to FINTRAC by the Compliance Officer whenever there are reasonable grounds to suspect that an activity is related to ML/TF. These reports must be submitted regardless of whether the transaction or activity is completed.

In order to reach the threshold for reasonable grounds to suspect, the Company does not need to know that there is a connection to a ML/TF offence, or even believe that such a connection exists. Reaching reasonable grounds to suspect means that the Company has considered all the facts, context, and ML/TF indicators related to a financial transaction and, after having reviewed this information, determined there is a reasonable possibility that the activity is related to ML/TF.

Refer to FINTRAC guidance as well as published ML/TF indicators for more information about determining suspicion.

The ultimate decision to file an STR is made by the Compliance Officer. Any potentially suspicious activity is escalated to the Compliance Officer for investigation.

At the time this document was published, existing FINTRAC STR schedules were unable to accept the new information reporting fields that were introduced as a result of the regulatory changes that came into force on June 1, 2021. As such, Brink's takes reasonable measures to obtain and keep record of non-mandatory information fields, until such time that the FINTRAC web reporting system is updated to accept such information.

[22] http://www.fintrac-canafe.gc.ca/reporting-declaration/form/TPR-2008-eng.pdf

[23] http://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide5/5-eng.asp#s55

Brink's maintains a copy of all STRs filed with FINTRAC (see Section 14).

### 12.3.1 IDENTIFICATION OF POTENTIALLY SUSPICIOUS ACTIVITY

Brink's identifies potentially suspicious activity through customer discussions with employees, transaction monitoring, as well as through communication with law enforcement.

#### A. EMPLOYEE INTERACTION

If through regular customer interaction, an employee suspects that a transaction may be related to a ML/TF offence, the employee must report it via the Company's internal Ethics hotline at +1-877-275-4585 (https://Brinkshotline.ethicspoint.com) or Brink's Compliance team's email address (BrinksCanadaKYC@brinks.com), prior to the end of the current working day. The Compliance Officer reviews and maintains a record of all unusual activity that is reported.

#### B. ONGOING MONITORING

Brink's has a process for reviewing transactions to identify potentially suspicious activity. Transactions are reviewed as described in Section 9.5.5.

#### C. COMMUNICATION WITH LAW ENFORCEMENT

Upon receiving a request from law enforcement, the Compliance Officer reviews the transaction history of the related customer for the previous two years to determine if there are reasonable grounds to suspect that the customer may have conducted or attempted to conduct transactions that are involved in a ML/TF offence.

### 12.3.2 INVESTIGATING SUSPICIOUS ACTIVITY

Upon becoming aware of a potentially suspicious activity, the Compliance Officer must review the transaction to determine if there are reasonable grounds to suspect that the transaction is related to an ML/TF offence.

In conducting their assessment as to whether there are reasonable grounds to suspect, the Compliance Officer must consider additional information sources such as the customer's transaction history, as well as customer characteristics and information (such as the PIN) that are contained in the customer's file. If required, the Compliance Officer may elect to contact the customer or employee to obtain additional information about the transaction.

After completing their review, the Compliance Officer should be comfortable:

- as to the legitimacy of the funds involved in the transaction;
- as to the identity of the parties involved in the transaction and the relationship between those parties;
- that the purpose of the transaction is not connected to criminal activity; and
- that none of the parties involved in the transaction have a connection to criminal activity.

If the Compliance Officer is not able to achieve this level of comfort, they likely have reached the threshold for establishing reasonable grounds to suspect a connection to ML/TF and should proceed with submitting an STR to FINTRAC as described in Section 12.3.4.

At the conclusion of the investigation, regardless of whether the Compliance Officer determines that there are reasonable grounds to suspect, a record is maintained describing the rationale for the Compliance Officer's decision. If the Compliance Officer determines that there are reasonable grounds to suspect, they must be able to clearly articulate the nature of their suspicion.

### 12.3.3 TIPPING OFF

If suspicion has arisen regarding a customer's identity or the legitimacy of a transaction, employees must not disclose information about the matter to anyone other than the Compliance Officer. This includes disclosing to a customer that an STR has been filed with FINTRAC in relation to one or more of the customer's transactions.

Informing anyone other than the Compliance Officer or a delegate about a suspicion may be considered a breach of the law.

### 12.3.4 STR SUBMISSION AND TIMEFRAME

The Compliance Officer reports attempted and completed suspicious transactions to FINTRAC as soon as is practicable after measures are taken to establish reasonable grounds to suspect that the activity is related to ML/TF.

Filing an STR with FINTRAC does not prevent reporting suspicions of ML/TF directly to law enforcement and FINTRAC encourages establishing and maintaining relationships with law enforcement.

The date that the Compliance Officer completed their investigation is used to document the date that they determined reasonable grounds for suspicion.

STRs are filed with FINTRAC electronically through the FINTRAC web reporting system.[24]

If the Company has submitted an STR to FINTRAC and needs to make a subsequent change to the report, it must make the change and submit the revised report to FINTRAC within 20 days of the date in which the Company made the request for change, based on system requirements. Brink's must also provide an explanation for the change.

### 12.3.5 POST REPORTING OBLIGATIONS

Once an STR has been filed, Brink's has the following post-reporting obligations:

- Keep reporting - the Company continues to report, as soon as reasonably practicable, subsequent transaction activity conducted by the customer that exhibits the same ML/TF indicators;
- Reassess risk - the Company reassesses the customer's risk rating, taking into consideration the STR filed;
- Review historical activity - previous transactions conducted by the customer are reviewed and an STR is submitted if those transactions have the same suspicious indicators; and

[24] https://www.fintrac-canafe.gc.ca/reporting-declaration/Info/f2r-eng

- Update Program - Brink's considers whether any updates to the Risk Assessment and/or Policies and Procedures are required, including updating the list of ML/TF indicators to include those resulting from the assessment and subsequent filing of suspicious transactions.

If the Company is reporting on the same person or entity, it can reference a previous STR in the Related Report(s) section by providing all of the following information:

- the reporting entity report reference number and the reporting entity transaction reference number;
- the reasonable grounds to suspect (facts, context, ML/TF indicators) that were included in the first STR submission; and
- any new additional information.

If Brink's is reporting STRs due to new facts, context, ML/TF indicators revealed during the assessment of the customer, they must detail this new information in the STR.

## 12.4 SANCTIONS EVASION REPORTS

Sanctions evasion offence means an offence arising from the contravention of a restriction or prohibition established by an order or a regulation made under the United Nations Act, SEMA or the Sergei Magnitsky Law.

Brink's must submit a STR to FINTRAC if there are reasonable grounds to suspect that a financial transaction that occurs or is attempted in the course of their activities is related to sanctions evasion. These transaction reports are critical to FINTRAC's ability to develop and disseminate financial intelligence.

### 12.4.1 IDENTIFICATION OF SANCTIONS EVASION

FINTRAC has published a special bulletin to help Reporting Entities identify characteristics of financial activity associated with suspected sanctions evasion.

Individuals and entities sanctioned by the Government of Canada are likely to deploy established techniques and channels to circumvent sanctions and use alternative financial channels should traditional methods be unavailable to them.

These techniques include the use of intermediary jurisdictions to set up complex networks of shell and front companies (often registered to addresses in offshore financial centres or tax havens) and non-resident bank accounts (generally located in secrecy jurisdictions or those known to cater to customers in sanctioned jurisdictions) as a key feature of sanctions circumvention. Some sanctioned individuals are also known to use trade-based money laundering and other techniques to move, hide, and use assets around the world.

Alternative financial channels—among them, cryptocurrencies and other emerging financial technologies—have also played an important role in sanctions circumvention activities.

Brink's must monitor its customer's activities to determine if there are reasonable grounds to suspect sanctions evasion. Refer to Section 12.3.1 for more information about how Brink's identifies suspicious transactions.

### 12.4.2 INVESTIGATING SANCTIONS EVASION

Refer to Section 12.3.2 for more details related to how Brink's investigates suspicious activity.

### 12.4.3 SUBMISSION OF A SANCTIONS EVASION STR

The Compliance Officer reports attempted and completed suspicious transactions to FINTRAC as soon as is practicable after measures are taken to establish reasonable grounds to suspect that the activity is related to sanctions evasion.

Filing an STR with FINTRAC does not prevent reporting suspicions of ML/TF directly to law enforcement and FINTRAC encourages establishing and maintaining relationships with law enforcement.

The date that the Compliance Officer completed their investigation is used to document the date that they determined reasonable grounds for suspicion.

STRs are filed with FINTRAC electronically through the FINTRAC web reporting system[25].

If the Company has submitted an STR to FINTRAC and needs to make a subsequent change to the report, it must make the change and submit the revised report to FINTRAC within 20 days of the date in which the Company made the request for change, based on system requirements. Brink's must also provide an explanation for the change.

Brink's has the same post reporting obligations related to sanctions evasion STRs as described in Section 12.3.5.

## 12.5 LARGE CASH TRANSACTION REPORTS

An LCTR is submitted to FINTRAC whenever the total of **all** cash received from or on behalf of the same individual or entity totals more than $10,000 or more or the equivalent value in a foreign currency within the Company's 24-hour period (see Section 12.1) and Brink's knows the transaction were:

- conducted by, or on behalf of the same person or entity;
- conducted on behalf of the same person or entity (third party); or
- for the same beneficiary.

Once an LCT has been received, an LCTR is submitted, even if transaction is suspended or rejected.

Refer to the FINTRAC website for details on the information that should be included in an LCTR[26].

Brink's maintains a copy of all LCTRs filed (see Section 14).

[25] https://www.fintrac-canafe.gc.ca/reporting-declaration/Info/f2r-eng
[26] http://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/1-eng.asp

### 12.5.1 LCTR SUBMISSION AND TIMEFRAME

LCTRs are submitted to FINTRAC electronically through the FINTRAC web reporting system[27] no later than 15 calendar days after the transaction occurred.

### 12.5.2 EXCEPTIONS TO REPORTING LARGE CASH TRANSACTIONS

The Company does have to report LCTs if the cash is received for transportation:

- to or from another reporting entity, if the transport is at their request and in an undeclared amount that cannot readily be determined;
- between the Bank of Canada and a person or entity in Canada; or
- between two places of business of another reporting entity, at their request.

Brink's does not have to submit an LCTR for the initiation of two or more cash transactions that total $10,000 or more under the 24-hour rule if the LCTs are initiated at the request of or on behalf of[28]:

  - a public body;
  - a financial entity; or
  - a person who is acting on behalf of a customer what is a public body or financial entity.

## 13. Voluntary Self-Declaration of Non-Compliance

FINTRAC recognizes that Reporting Entities may come across instances where they have not met all the requirements of the Legislation. A situation of non-compliance is a violation or series of minor violations of the PCMLTFA in relation to reporting, customer identification, recordkeeping, or effectively implementing an area of the Program.

Brink's has adopted the PCMLTFA Administrative Monetary Penalties Regulations guidance on the severity of violations in order to determine a "significant" situation of non-compliance, which is defined as:

- 50 minor violations;
- more than two serious violations; or
- one very serious violation.

Generally, Brink's submits a Voluntary Self-Disclosure of Non-Compliance ("VSDONC") to FINTRAC whenever it has identified a situation of significant non-compliance, unless:

- the Company has received notification of an upcoming examination; or,
- a similar VSDONC has been filed, or FINTRAC would otherwise be aware of the non-compliance.

A situation of non-compliance can be identified in the course of day-to-day operations, during the course of an effectiveness review, or other quality control activities. All situations of non-compliance

[27]https://www.fintrac-canafe.gc.ca/reporting-declaration/Info/f2r-eng
[28] This exception does not apply in the case of a single cash transaction of $10,000 or more. Brink's must submit an LCTR when a single transaction that amounts to $10,000 or more is conducted under the 24-hour rule if the LCTs are initiated at the request of or on behalf of a public body; or a financial entity; or a person who is acting on behalf of a customer what is a public body or financial entity.

are escalated to the attention of the Compliance Officer who determines whether a VSDONC is to be filed.

VSDONCs are submitted without delay to FINTRAC via email to VSDONC.ADVNC@fintrac-canafe.gc.ca and include the following information:

- the name and the contact details of the individual submitting the VSDONC;
- for reporting issues: the number of reports impacted, type, and the time period during which the issues occurred, as well as the reason why the reports were not submitted, were late, or incorrect, and other related details;
- for other issues: the period of time during which the issues occurred, the reason for their occurrence; and
- a plan to resolve the issues and submit all outstanding (or incorrect/incomplete) reports, including measures and timelines for corrective action.

Brink's only provides FINTRAC with the required information. Personal or protected information related to employees or customers must not be included, unless specifically requested by FINTRAC.

## 14. RECORDKEEPING

Brink's is required to have procedures in place for keeping records of pertinent information. Records can be kept in an electronic form, as long as a paper copy can be readily produced from them, and records are kept in such a way that they can be provided within 30 days of a request to examine them.

In support of that requirement, Brink's keeps all associated records in accordance with the timeframes detailed in the chart below.

| Record to be Kept | Contents of Record | Time Period and Location |
|---|---|---|
| AML program details | • all Program documents, including policies, procedures, and Risk Assessment, as well as records of the changes to the Program;<br>• compliance effectiveness review reports and any associated action plan, including appropriate sign-off on the final report;<br>• a record of the content, date, and completion/attendance of any AML/CTF related training sessions; and<br>• all FINTRAC correspondence. | Five years after the report/ training/ correspondence date at Head Office, electronically |
| Customer information | • all customer identification records (see Section 9.3);<br>• all PEP determination and related records (see Section 9.6.2);<br>• all records related to EDD measures for high-risk customers (see the Risk Assessment); | Five years after the business relationship ceases, or where there is no business relationship, five years after the |

| | | |
|---|---|---|
| | • all information collected as part of the customer risk assessment (see the Risk Assessment);<br>• all records of the PIN for business relationships (see Section 9.5.2);<br>• records of the measures taken to monitor business relationships and the information obtained as a result of ongoing monitoring (see Section 9.5.6); and<br>• records of all Service Agreements (see Section 9.2.4). | record was created, at Head Office, electronically |
| Internal memos | An internal memorandum means any memo, note, message, or similar communication that is created or received, in the normal course of business, about services provided to customers. | Five years after the record has been created at Head Office, electronically |
| UTR records | A record of:<br>• whether the transaction was reported to FINTRAC;<br>• the Compliance Officer's investigation process;<br>• a rationale describing why the transaction or attempted transaction was or was not reported to FINTRAC; and<br>• a copy of the UTR, as applicable. | Five years after the report is made at Head Office, electronically |
| STR records | A copy of all STRs submitted to FINTRAC, along with the date of submission, including sanctions evasion STRs. | Five years after the report is made at Head Office, electronically |
| TPR records | A copy of all TPRs submitted to FINTRAC, the RCMP, and CSIS, along with the date of submission. | Five years after the report is made at Head Office, hard copy |
| LCTR records | All LCTRs submitted to FINTRAC. | Five years after the record is created, at Head Office, electronically |
| VSDONC records | If a VSDONC is submitted to FINTRAC:<br>• a copy of the VSDONC that was submitted to FINTRAC along with any emails sent to or received from FINTRAC with respect to the non-compliance;<br>• all supporting documentation related to the issue; and<br>• the resolution plan and corrective actions taken. | Five years after the report is made at Head Office, electronically |
| Records for the transportation of $3,000 or more in money orders, traveller's | If Brink's transports $3,000 or more in money orders, traveller's cheques, or other similar negotiable instruments, the Company maintains a record of:<br>• the date and location of collection and delivery,<br>• the type and amount of cash, virtual currency or negotiable instruments transported, | Five years after the record is created, at Head Office, electronically |

| | | |
|---|---|---|
| cheques, or other similar negotiable instruments (except cheques payable to a named person or entity) | • the name and address of the person or entity that made the request, the nature of their principal business or their occupation and, in the case of a person, their date of birth,<br>• the name and address, if known, of each beneficiary,<br>• the number of every account that is affected by the transport, the type of account and the name of each account holder,<br>• every reference number that is connected to the transport and has a function equivalent to that of an account number, and<br>• the method of remittance<br>• | |
| Records for transporting cash of $1,000 or more | When Brink's transports cash of $1,000 or more, **at the request of a person or entity**, the Company maintains a record of:<br>• the date and location of the collection and delivery;<br>• the type of amount of cash transported;<br>• customer name, address, telephone number, occupation/nature of principal business, and date of birth (if an individual) for any person or entity that made the request;<br>• the name and address, if known, of each beneficiary;<br>• the number of every account affected by the transport, the type of account, and the name of the account holder;<br>• every reference number that is related to the transport that has a function equivalent to that of an account number; and<br>• the method of remittance. | Five years after the record is created, at Head Office, electronically |
| Records for transporting undisclosed or undeterminable amounts of cash, money orders, traveller's cheques or other negotiable instruments (except | When Brink's transports undisclosed or undeterminable amounts of cash, **at the request of a person or entity**, the Company maintains a record of:<br>• the date and location of the collection and delivery;<br>• the type of cash transported (if known);<br>• customer name, address, telephone number, occupation/nature of principal business, and date of birth (if an individual) for any person or entity that made the request;<br>• the name and address, if known, of each beneficiary;<br>• the number of every account affected by the transport, the type of account, and the name of the account holder; | Five years after the record is created, at Head Office, electronically |

| | | |
|---|---|---|
| cheques payable to a named person or entity) | • every reference number that is related to the transport that has a function equivalent to that of an account number; and<br>• the method of remittance; and<br>• the reason the amount was not declared. | |
| Transporting cash, money orders, traveller's cheques or other negotiable instruments (except cheques payable to a named person or entity) to a named person or entity | If cash is being transported to a name person or entity, **at the request of an entity**, the Company maintains a record of:<br>• the date and location of collection and delivery;<br>• the type and amount, if known, of the cash; and<br>• the name, address and telephone number of the entity that made the request. | Five years after the record is created, at Head Office, electronically |
| LCT records | Brink's maintains a record of each LCT, which includes the following information:<br>• the date of the cash is received;<br>• the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or occupation and, in the case of an individual, their date of birth;<br>• the type and amount of each fiat currency involved in the receipt;<br>• the method by which the cash is received;<br>• the exchange rate used and the source of the rate (if applicable);<br>• every reference number that is connected to the transaction and has a function equivalent to that of an account number; and<br>• the purpose of the transaction. | Five years after the record is created, at Head Office, electronically |
| Third-party determination records | <u>If a third party is suspected (unconfirmed)</u><br>If Brink's suspects that there is a third party, but is unable to make a third-party determination:<br>• the reason the Company suspects that the customer is acting on behalf of a third party; and<br>• whether the customer indicated that they were acting on behalf of a third party; and<br>• any additional measures that were taken to make the determination<br><u>All other third-party determinations:</u> | Five years after the determination is made at Head Office, electronically |

| | | |
|---|---|---|
| | • all records of third-party determinations that have been made; and<br>• all records of identified third-party relationships. | |
| Reasonable measures | In instances where Brink's is required to take reasonable measures, and those measures are unsuccessful, the Company keeps a record to demonstrate that those measures were completed, such as the date the measure was taken, what measures were taken, and the reason the measures were unsuccessful. | Five years after the determination is made at Head Office, electronically |

## 14.1 EXCEPTIONS TO RECORD KEEPING

The Company is not required to keep an LCT record if the cash is received for transportation:

- to or from another reporting entity, if the transport is at their request and in an undeclared amount that cannot readily be determined;
- between the Bank of Canada and a person or entity in Canada; or
- between two places of business of another reporting entity, at their request.

Brink's is not required to keep any Service Agreement records (including information records) when the Company enters into a Service Agreement with an entity **only** for the transport of cash, or money orders, traveller's cheques, or similar negotiable instruments between:

- the Bank of Canada and a person or entity in Canada;
- two financial entities; or
- two places of business of a reporting entity, at their request.

The same Service Agreement exception applies when the Company enters into a Service Agreement with an entity only for the transportation of coins of the currency of Canada that are produced or supplied by the Royal Canadian Mint that are delivered to the Minister of Canada (or to a person designated by the Minister of Finance).

Brink's is not required to keep transport records when the Company transports cash, money orders, traveller's cheques, or other similar negotiable instruments between:

- the Bank of Canada and a person or entity in Canada;
- two financial entities; or
- two places of business of a reporting entity, at their request.

The same exception applies in respect of the transportation of coins of the currency of Canada that are produced or supplied by the Royal Canadian Mint that are delivered to the Minister of Canada (or to a person designated by the Minister of Finance).

## 14.2 RECORDING CUSTOMER OCCUPATION

When Brink's records a customer's occupation or nature of principal business, the Company needs to be as descriptive as possible. In addition to documenting the customer's job title, the Company must be sure to obtain details regarding the specific type of work and industry. As a rule of thumb, the occupation or nature of principal business should be documented in such a way that another person who reads the customer record has an understanding of what the customer does for a living.

The following table provides examples of acceptable and unacceptable descriptions of customer occupation and nature of principal business.

| Acceptable Descriptions | Insufficient Descriptions |
|---|---|
| Individual Customers | |
| Doctor - Cardiologist | Doctor |
| Machine Operator - Electronics Manufacturing | General Labourer |
| Vehicles Sales | Sales |
| Self-employed Cabinet Maker | Self-employed |
| Entity Customers | |
| Manufacturing of Industrial Equipment | Manufacturing |
| Management Consulting | Consulting |
| Importing of Clothing from Overseas | Importing |
| Securities Dealer, Credit Union, Money Services Business, Payment Service Provider, etc. | Financial Services |

## 15. Procedure Approval and Change Log

| Version | Date Approved | Explanation of Changes/Updates | Approver Name and Title |
|---|---|---|---|
| 1.0 | July 1, 2024 | Development of Anti-Money Laundering/Counter- Terrorism Financing Compliance Policies and Procedures. | Rachel Moon, VP and AML Officer |

| **Senior Management Acknowledgement of Changes – Reviewed and Approved by:** | | | |
|---|---|---|---|
| Senior Manager name: | Rachel Moon | | |
| Senior Manager Title: | VP and AML Officer | Date of Approval: | July 1,2024 |

# APPENDIX A – APPOINTMENT OF DESIGNATED COMPLIANCE OFFICER

Brink's has appointed the following individuals to the position of the Compliance Officer and back-up Compliance Officer effective to the position articulated in Section 8.2.

| | **Compliance Officer** | **Back-up Compliance Officer** |
|---|---|---|
| Name | Rachel Moon | N/A |
| Position | VP and AML Officer | |
| Date appointed | 03/15/2024 | |
| Appointed by | Senior Management | |
| Date approved | 03/15/2024 | |
| Approved by | Senior Management | |

## APPENDIX B – SAMPLE TRAINING LOG

| Employee name | Date of hire | Type of training delivered | Date of training delivery | Date of training completion |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

SAMPLE

# APPENDIX C – SAMPLE THIRD-PARTY DETERMINATION FORM

Brink's takes reasonable measures to determine whether a customer is acting on behalf of a third party:

- When Brink's receives $10,000 or more in cash for transport, unless the Company is exempt from filing an LCTR (see Section 12.5) or keeping records (see Section 14) in respect of that transaction; and
- upon entering into a Service Agreement.

**Third-Party Definition**

"Third-party" means an individual or entity other than the individual who conducts the transaction. It is not about who owns the money, but rather about who gives instructions to deal with the money. If the individual is acting on someone else's instructions, that someone else is the third-party. When employees are acting on behalf of their employers, they are considered to be acting on behalf of a third-party.

**Reasonable Grounds to Suspect Third-Party Involvement**

In situations where Brink's is unable to determine third-party involvement but there are reasonable grounds to suspect that there are instructions of a third-party involved, the sales representative must document the following information and include it with the customer's information to be sent to Compliance for review.

I. Whether, according to the customer, the transaction is being conducted on behalf of a third-party.
II. Details as to why you suspect the individual is acting on a third-party's instructions.

**Third-Party Record**

| **Question/Information** | **Response** |
|---|---|
| Are you acting on behalf of or the for the benefit of a third-party? | ☐ **YES** ☐ **NO** |
| **If the customer answers YES, they must provide the following:** | |
| Third-party's full name | |
| Third-party's full address | |
| Third-party phone number | |
| Third-party's principal business or occupation | |
| Third-party's date of birth (if individual) | |
| Third-party's incorporation number and place of incorporation (if corporation) | |
| The nature of the relationship between the third-party and the customer | |
| Other comments/suspicions of third-party involvement | |

If Brink's is unsuccessful in determining whether a customer was acting on behalf of a third party, but there are reasonable grounds to suspect that a third party is instructing the customer, Brink's must record:

| **Information** | **Response** |
|---|---|
| The steps taken to make the third-party determination | |
| The reason(s) Brink's was unsuccessful | |
| The date these steps were taken | |

# APPENDIX D – PEP AND HIO DEFINITIONS

A PEP or HIO is a person entrusted with a prominent position that typically comes with the opportunity to influence decisions and the ability to control resources. The influence and control that a PEP or HIO has can make them vulnerable to corruption.

**Foreign PEP**

A foreign PEP is a person who holds or has held one of the following offices or positions in or on behalf of a foreign state:

- Head of state or head of government
- Member of the executive council of government or member of a legislature
- Deputy minister or equivalent rank
- Ambassador, or attaché or counsellor of an ambassador
- Military officer with a rank of general or above
- President of a state-owned Company or a state-owned bank
- Head of a government agency
- Judge of a supreme court, constitutional court, or other court of last resort
- Leader or president of a political party represented in a legislature

**Domestic PEP**

A domestic PEP is a person who holds—or has held within the last five years—a specific office or position in or on behalf of the Canadian federal government, a Canadian provincial government, or a Canadian municipal government.

- Governor General, lieutenant governor, or head of government
- Member of the Senate or House of Commons or member of a legislature
- Deputy minister or equivalent rank
- Ambassador, or attaché or counsellor of an ambassador
- Military officer with a rank of general or above
- President of a corporation that is wholly owned directly by Her Majesty in right of Canada or a province
- Head of a government agency
- Judge of an appellate court in a province, the Federal Court of Appeal, or the Supreme Court of Canada
- Leader or president of a political party represented in a legislature
- Mayor, reeve, or other similar chief officer of a municipal or local government 29

**HIO**

An HIO is either:

- the head of an international organization established by the governments of states;
- the head of an institution established by an international organization; or

[29] In line with legislation across Canada, municipal governments include cities, towns, villages and rural (county) or metropolitan municipalities. As such, a mayor is the head of a city, town, village and rural or metropolitan municipality, regardless of the size of the population.

- the head of an international sports organization.30

In making its determination, the Company takes into consideration that the head of an international organization is the primary person who leads that organization, e.g., a president or CEO.

**Family Members of PEP and HIO**

In determining the PEP status of its customers, the Company takes into consideration whether the customer is a family member of a PEP or HIO.

The following individuals are recognized as PEP or HIO by virtue of their family relationship:

- the spouse or common-law partner of a PEP or HIO;
- the biological or adoptive child of a PEP or HIO;
- the mother or father of a PEP or HIO;
- the mother or father of a spouse or common-law partner of a PEP or HIO; or
- the sibling of a PEP or HIO; or
- the ex-spouse or ex-common-law partner of a PEP or HIO.

**Close Associates of a PEP and HIO**

In determining the PEP status of its customers, the Company takes into consideration if the customer is a close associate of a foreign PEP, domestic PEP, or HIO.

The term "close associate" is not intended to capture every person who has been associated with the PEP or HIO. At a minimum, the Company determines the following persons to be close associates:

- in a romantic relationship with a PEP or HIO, such as a boyfriend, girlfriend, or mistress;
- involved in financial transactions with a PEP or HIO;
- business partners with, or who beneficially owns or controls a business with, a PEP or HIO;
- a prominent member of the same political party or union as a PEP or HIO;
- serving as a member of the same board as a PEP or HIO; or
- closely carrying out charitable works with a PEP or HIO.

Should the Company identify a customer's relationship with a PEP or HIO that is not included in this relationship list, the Compliance Officer determines whether they fit the definition of a close associate based on whether there is an apparent business or financial connection between the parties.

[30] https://www.fintrac-canafe.gc.ca/guidance-directives/customer-customerele/pep/pep-eng#s3

## APPENDIX E – SAMPLE PEP APPROVAL FORM

# Politically Exposed Person* Approval Form

| |
|---|
| Customer Reference # _____ Date Identified as a PEP _____ |
| First Name _____ Last Name _____ |
| Duration of Relationship _____ Nationality _____ |
| Office or position of the PEP _____ |
| Name of the Organization or Institution of the PEP _____ |
| Country of the Organization or Institution _____ |
| The relationship to the PEP, if customer is not the PEP themselves _____ |
| The source of wealth _____ _____ |
| Additional information related to transactions:<br>The source of funds that were used for the transaction (if required) _____ |
| Reviewed by (Senior Management) (if required): _____ |
| Date Reviewed: _____ |

*Reference to a PEP, for the purposes of the current regulatory framework, includes reference to a domestic PEP, foreign PEP, HIO, or a prescribed family member or close associate of one of these persons.