Section 1 - Overview & PIA Initiation

Government Institution: Royal Canadian Mint (Mint)

Official Responsible for the PIA
Simon Kamel
Vice President, General Counsel and Corporate Secretary,
Corporate and Legal Affairs

Head of the government institution or Delegate for section 10 of the *Privacy Act*
Emily-Brynn Rozitis
Senior Program Manager, Privacy
Corporate and Legal Affairs

Name of Activity: Know Your Agent (KYA), Know Your Customer (KYC) & Know Your Supplier (KYS); collectively "Due Diligence Activities"

Description of the class of record and personal information bank:
Institution specific class of record:
Due Diligence Compliance Activities - RCM 1520
Institution specific personal information bank:
Under Development

Legal Authority for activity:
The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA); the *Corruption of Foreign Public Officials Act* (CFPOA) and their associated regulations; and the *Royal Canadian Mint Act*.

Description Summary:
The Mint's KYA, KYC & KYS activities ("Due Diligence Activities") ensure that customers, precious metals suppliers and agents acting on behalf of the Mint undergo an appropriate level of due diligence prior to the completion of any precious metals sales, refining and storage transactions. The Mint's Due Diligence Activities involve the collection, use and disclosure of personal information (as defined in section 3 of the *Privacy Act*) directly from members of the public (including individuals, sole proprietors and representatives of entities), as well as the indirect collection of personal information in certain instances. The Due Diligence Activities are crucial processes to ensure that all of the Mint's existing and prospective customers (with the exception of select categories of numismatic customers consistent with the Mint's risk-based approach), agents and certain transportation companies in the customers' respective supply chains, are known with respect to their true identities and business activities with the intended outcome of securing sound business relationships and maintaining the Mint's reputational integrity.

The Mint is also committed to ensuring that every reasonable effort is made to detect and deter money laundering and terrorist financing activity through its business lines. The Mint therefore requires all of its precious metal refining customers and suppliers to do their part in ensuring that materials they bring in for processing are not sourced from conflict-affected or high-risk areas. By requiring all customers and suppliers of precious metals to participate in the Mint's Responsible Metals Program aimed at identifying and validating the supply chain of all incoming gold or silver-bearing refining deposits, the Mint advances responsible business practices and promotes the responsible sourcing of precious metals used in its processes and products.

PIA Scope:
The scope of the PIA includes a review of the internal privacy practices associated with the Due Diligence Activities policies and related business processes, the basic data flows of personal information, and the management and safeguarding of this information by the Mint in support of the organization's compliance activities. As such, lawful disclosure requirements to regulatory bodies and/or law enforcement and same's handling of reporting information upon receipt, in addition to any future potential developments in relation to technological and electronic systems and methods, are outside the scope of this PIA. As PIAs are evergreen documents, the Mint commits to revisiting the report's content in the event of substantive changes to the personal information management practices associated with the Due Diligence Activities.

Section 2 - Risk identification and categorization

The following section contains standardized risks identified in the PIA report per the TBS requirements for a core PIA. The common, numbered risk scale is utilized where appropriate in ascending order: the first level (1) represents the lowest level of potential risk for the risk area; the fourth level (4) represents the highest level of potential risk for the given risk area.

A) Type of program or activity

Risk scale - 2: Administration of program or activity and services.

Risk scale - 3: Compliance or regulatory investigations and enforcement.

B) Type of personal information involved and context

Risk scale – 3: Social Insurance Number, medical, financial or other sensitive personal information or the context surrounding the personal information is sensitive; personal information of minors or of legally incompetent individuals or involving a representative acting on behalf of the individual.

Risk scale – 4: Sensitive personal information, including detailed profiles, allegations or suspicions and bodily samples, or the context surrounding the personal information is particularly sensitive.

C) Program or activity partners and private sector involvement

Risk scale – 2: With other government institutions; and

Risk scale - 4: Private sector organizations, international organizations or foreign governments.

D) Duration of the program or activity:

Risk scale – 3: Long-term activity.

E) Program population

Risk scale – 3: The program's use of personal information for external administrative purposes affects certain individuals.

F) Technology & privacy

Does the new or modified program or activity involve the implementation of a new electronic system, software or application program including collaborative software (or groupware) that is implemented to support the program or activity in terms of the creation, collection or handling of personal information?

No

Does the new or modified program or activity require any modifications to IT legacy systems and/or services?

No

The new or modified program or activity involves the implementation of one or more of the following technologies:

Enhanced identification methods?

No

Use of Surveillance?

No

Use of automated personal information analysis, personal information matching and knowledge discovery techniques?

No

G) Personal information transmission

Risk scale – 2: The personal information is used in a system that has connections to at least one other system.

Risk scale – 4: The personal information is transmitted using wireless technologies.

H) Risk impact to the individual or employee

Risk scale – 1: Inconvenience.

Risk scale – 2: Reputation harm, embarrassment.

Risk scale – 3: Financial harm.