Summary of Privacy Impact Assessment
Payout Modernization Initiative – 2023

Government institution:

Canada Deposit Insurance Corporation ("**CDIC**" or the "**Corporation**")

Head of government institution or delegate:

Christa Walker, Chief Legal Officer, Corporate Secretary, Head, Policy Integration and ATIP Coordinator

Senior official or executive for the new or substantially modified program or activity:

Michael Mercer, Chief Data & Insurance Officer

Name of program or activity of the government institution:

Payout Modernization Initiative

Overview and Background

Under section 7 of the CDIC Act, CDIC's statutory objects are:

a) to provide insurance against the loss of part or all of deposits;

b) to promote and otherwise contribute to the stability of the financial system in Canada;

c) to pursue the objects set out in paragraphs (a) and (b) for the benefit of persons having deposits with member institutions and in such manner as will minimize the exposure of the Corporation to loss; and

d) to act as the resolution authority for its members.

In furtherance of CDIC's objects, and pursuant to the CDIC Act, CDIC insures each depositor at a member institution ("**MI**") for the value of eligible deposits to a maximum of $100,000 per deposit insurance category. For more information about the different categories of deposit insurance coverage, please see CDIC's website. Where a MI fails, CDIC is required to make payment in respect of all deposits insured by deposit insurance to such person as CDIC determines is entitled. This payment must be made as soon as possible after the obligation arises.

To determine the amounts owing to insured depositors, deposit information is extracted by the MIs from their internal systems, submitted to CDIC and loaded into CDIC's payout application(s). The payout application(s) then organize(s) the deposit information to allow CDIC to determine the amount of the payments to be issued to insured depositors. To make an insurance determination and issue those payments, CDIC must collect, use and disclose personal information of depositors of the failed MI.

To support efficient and effective payout processes, CDIC is engaging in a multi-stage payout modernization initiative (the "**Initiative**") that will improve CDIC's ability to provide insured depositors with access to funds in a timely, accurate and efficient manner. To achieve the objectives of the Initiative, CDIC plans to enhance the technology for data management and robustness, depositor communication protocols and systems, payout applications and processes, and the premium calculation process.

This PIA focuses on the first phase of the Initiative which is focused on enhancing internal CDIC functionality. It builds a higher degree of automation of data compliance and insurance determination processes in a secure cloud environment.

Legal Authority

In addition to the general authority in Sections 7 and 14 of the *Canada Deposit Insurance Corporation Act* (the "**CDIC Act**"), CDIC's legal authority to collect, use and disclose personal information for compliance purposes is also founded under Section 2(1)(a)(ii) of the CDIC *Data and System Requirements By-Law* (the "**DSRB**") for MIs. The *Co-Owned and Trust Deposit Disclosure By-Law* ("**COTDB**") as well as Section 7(1) of the Schedule to the CDIC Act (the "**Schedule**") governs the process for the NBs.

As it pertains to MIs, the DSRB provides CDIC with the authority to collect (and to require a MI to provide within 6 hours after end of day processing following CDIC's request) the following information:

- unique depositor
- eligibility to be insured by the Corporation
- insurance
- account type
- any other information specified in the DSRB respecting the insured deposit.

The secure file transfer protocol ("**SFTP**") serves as a medium to transfer information to CDIC pursuant to the DSRB.

As it pertains to nominee brokers ("**NB**s"), Section 7(1)(b) of the Schedule provides CDIC with the authority to collect (and to require a NB to provide within three (3) business days of CDIC's request) the following information:

- each unique alphanumeric code for each beneficiary (unique client identifier- UCI) of the deposit held by a member institution in the name of the NB;
- the current name and address of the beneficiary associated with that code, and
- any other information specified in the by-laws respecting the deposit.

The CDIC broker portal serves as a medium to transfer information to CDIC pursuant to the COTDB as referenced in Section 7(1)(a) of the Schedule.

Contract with Service Provider

CDIC is authorized to engage service providers to assist it in executing its objects under the CDIC Act – both inherently under its general authority noted above, but also pursuant to subsection 10(1) of the CDIC Act, which permits CDIC to do all things necessary or incidental to the objects of the Corporation.

Personal Information Banks ("PIBs")

The collection and use of personal information for the Initiative is within the scope of the following PIB:

- "Deposit and Beneficiary Records" (Bank Number: CDI PPU 005) applies to the personal information of depositors.

Risk Area Identification and Categorization

The Directive on Privacy Impact Assessment sets out a risk identification and categorization matrix. The numbered risk scale is presented in an 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. CDIC has highlighted in bold the risk assessment applicable to the Initiative.

Type of program or activity	Risk scale
Program or activity that does NOT involve a decision about an identifiable individual	1
Administration of program or activity and services	2
Compliance or regulatory investigations and enforcement – *CDIC explanation: The Initiative collects personal information to assess whether MIs and NBs are in compliance with applicable CDIC regulations and by-laws, as well as to determine the value of insured deposits held by CDIC MIs.*	**3**
Criminal investigation and enforcement or national security	4

Type of personal information involved and context	Risk scale
Only personal information, with no contextual sensitivities, collected directly from the individual or provided with the consent of the individual for disclosure under an authorized program.	1
Personal information, with no contextual sensitivities after the time of collection, provided by the individual with consent to also use personal information held by another source.	2
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. – *CDIC explanation: Among other personal information, the Initiative involves financial information about identifiable individuals.*	**3**
Sensitive personal information, including detailed profiles, allegations or suspicions and bodily samples, or the context surrounding the personal information is particularly sensitive.	4

Program or activity partners and private sector involvement	Risk scale
Within the institution (among one or more programs within the same institution)	1
With other government institutions	2
With other institutions or a combination of federal, provincial or territorial, and municipal governments	3
Private sector organizations, international organizations or foreign governments – *CDIC explanation: This Initiative involves the collection of personal information from MIs and NBs (private sector organizations) as authorized by CDIC's bylaws. The Initiative also relies on private sector organizations to provide cloud and related IT services to host and process personal information.*	**4**

Duration of the program or activity	Risk scale
One-time program or activity	1
Short-term program or activity	2
Long-term program or activity – *CDIC explanation: The Initiative is intended as a long-term program or activity.*	**3**

Program population	Risk scale
The program's use of personal information for internal administrative purposes affects certain employees.	1
The program's use of personal information for internal administrative purposes affects all employees.	2
The program's use of personal information for external administrative purposes affects certain individuals – *CDIC explanation: The Initiative involves using personal information of insured depositors and beneficiaries provided by CDIC's MIs and NBs to assess compliance and determined insured amounts.*	**3**
The program's use of personal information for external administrative purposes affects all individuals.	4

Technology and privacy	Risk scale
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?	Yes
Does the new or modified program or activity require any modifications to IT legacy systems and/or services?	Yes
Does the new or modified program or activity involve the implementation of one or more of the following technologies: • enhanced identification methods; • surveillance; or • automated personal information analysis, personal information matching or knowledge discovery techniques.	 Yes Yes Yes

Personal information transmission	Risk scale
The personal information is used within a closed system.	1
The personal information is used in a system that has connections to at least one other system.	2
The personal information is transferred to a portable device (i.e., USB key, diskette, laptop computer), transferred to a different medium or is printed.	3
The personal information is transmitted using wireless technologies – *CDIC explanation: The Initiative involves the use of CDIC's internal systems. It also includes the transmission of files containing personal information using wireless technology*.	**4**

Potential risk that in the event of a privacy breach, there will be an impact on the individual or employee.	Risk scale
Inconvenience	Yes
Reputation harm, embarrassment	Yes
Financial harm	Yes
Physical harm	No

CDIC explanation: CDIC has implemented measures to mitigate such risks by restricting access to personal information to authorized personnel only and limiting the personal information shared with MIs and NBs for compliance purposes.

Potential risk that in the event of a privacy breach, there will be an impact on the institution. *CDIC explanation: If there is a privacy breach related to the portal, the breach would have an impact on CDIC's reputation.*	**Risk scale**
Managerial harm – Processes must be reviewed, tools must be changed, change in provider / partner.	Yes
Organizational harm – Changes to the organizational structure, changes to the organizations decision-making structure, changes to the distribution of responsibilities and accountabilities, changes to the program activity architecture, departure of employees, reallocation of HR resources.	Yes
Financial harm – Lawsuit, additional moneys required reallocation of financial resources.	Yes
Reputation harm, embarrassment, loss of credibility - Decrease confidence by the staff, public, elected officials under the spotlight, institution strategic outcome / payout effectiveness compromised, impact on stability of financial system.	Yes

CDIC explanation: CDIC has implemented measures to mitigate such risks by restricting access to personal information to authorized personnel only and limiting the personal information shared with MIs and NBs for compliance purposes.

Categorization of risks using a common risk scale	**Risk scale**
The following table summarizes the results of the standardized risk assessment above:	
No. of program characteristics identified as "low" risk (TBS Level 1)	0
No. of program characteristics identified as "moderate" risk (TBS Level 2 or 3)	4
No. of program characteristics identified as "elevated" risk (TBS Level 4)	2
Overall risk rating for the portal	Moderate

Based on a summary analysis of program characteristics, the portal, in general, is likely to present a moderate risk to the privacy of individuals.