Summary of Payout Modernization Privacy Impact Assessment – 2021

Government institution:
Canada Deposit Insurance Corporation (CDIC)

Head of government institution or delegate:
Christa Walker, General Counsel, Corporate Secretary & Chief Legal Officer 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

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 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 at: **https://www.cdic.ca/your-coverage/how-deposit-insurance-works/**. Where a member institution 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.

In order to make payments of deposit insurance, CDIC must collect, use and disclose certain personal information of depositors in a failed member institution. To support efficient and effective payout processes, CDIC intends to modernize its payout systems. The first step to this modernization process is the creation of a

portal. The PIA focuses on creating such a portal for use by nominee brokers and professional trustees to submit personal information for compliance and payout purposes.

Legal Authority

In addition to the general authority in sections 7 and 14 of the Canada Deposit Insurance Corporation Act, and once certain amendments to the CDIC Act come into force, CDIC's legal authority to collect, use and disclose personal information for compliance purposes will also be founded in subsection 7(1)(b) of the Schedule to the CDIC Act That subsection will provide CDIC with the authority to collect (and to require a nominee broker to provide within 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 broker;
- 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 portal serves as a medium to transfer information to CDIC pursuant to the (not yet in force) Co-owned Trust and Deposit By-law That By-law requires nominee brokers to provide CDIC with additional information pursuant to subsection 7(1)(b) of the Schedule to the CDIC Act.

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 all things necessary or incidental to the objects of the Corporation.

Personal Information Banks ("PIBs")

The collection and use of personal information by the portal is within the scope of two existing PIBs.

- "Deposit and Beneficiary Records" (Bank Number: CDI PPU 005) applies to the personal information of depositors.
- "Electronic Network Monitoring Logs" (Bank Number: PSU 905) applies to the personal information contained in the network logs of CDIC's electronic networks It encompasses portal usage data for individual nominee broker users, professional trustee users and CDIC users.

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.

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 – *CDIC explanation: The portal is a communications channel, to facilitate the secure exchange of information between nominee brokers/professional trustees and CDIC.*	**2**
Compliance or regulatory investigations and enforcement	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: The portal acts as an interface to allow for the collection and transfer of financial information about beneficiaries who are 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: The portal will involve a private sector service provider that will permit the transmission of data between CDIC and nominee brokers/trustees, and the short-term hosting of that data on service provider systems.*	**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 portal is intended as a longer term arrangement for compliance purposes; however, the only personal information obtained for a long-term is usage information (External user account profile and External user information), cases and attestation responses. UCIs are only retained for a short period of time per CDIC's internal retention policies.*	**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 portal affects individual beneficiaries of accounts at CDIC member institutions.*	**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.	 No No No

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 – *CDIC explanation: The portal involves CDIC's secure internal system and service provider systems.*	**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.	4

Potential risk that in the event of a privacy breach, there will be an impact on the individual or employee.	Risk scale
Inconvenience	1
Reputation harm, embarrassment	**2**
Financial harm	3
Physical harm	4

CDIC explanation: As no personal information of beneficiaries (name, address, financial information about their beneficial interest in a deposit) except UCIs are retained on the portal, the only other personal information that could be breached is usage information.

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.	1
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.	2
Financial harm – Lawsuit, additional moneys required reallocation of financial resources.	3
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.	**4**

CDIC explanation: The breach could damage CDIC's reputation, which could undermine CDIC's ability to carry out its objects.

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)	6
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.