B.1.2 Notice of Agreement Concerning the Sharing of Derivatives Data Between the Ontario Securities Commission and Bank of Canada

NOTICE OF AGREEMENT
CONCERNING THE SHARING OF DERIVATIVES DATA BETWEEN
THE ONTARIO SECURITIES COMMISSION
AND
BANK OF CANADA

On February 19, 2025, the Ontario Securities Commission (**OSC**) entered into an agreement concerning the sharing of derivatives data with the Bank of Canada (the **Agreement**).

The Agreement provides for the Bank of Canada to receive certain data from the OSC for the purposes of supporting its goal of maintaining overall financial stability in Canada. The terms of the Agreement outline conditions and procedures for the transmission and use of the shared data.

Questions may be referred to:

Greg Toczylowski
Manager, Trading & Markets – Derivatives
Ontario Securities Commission
416-593-8215
gtoczylowski@osc.gov.on.ca

AGREEMENT

CONCERNING THE SHARING OF DERIVATIVES DATA

BETWEEN

BANK OF CANADA

AND

ONTARIO SECURITIES COMMISSION

AGREEMENT CONCERNING THE SHARING OF DERIVATIVES DATA (the "**Agreement**")

BETWEEN

BANK OF CANADA, (the "**Bank**"),

AND

ONTARIO SECURITIES COMMISSION, (the "**OSC**"),

each a "**Party**", and collectively referred to as the "**Parties**".

RECITALS:

A. The OSC collects information and data on securities and derivatives transactions in the Province of Ontario as part of its regulatory oversight function.

B. The Bank of Canada is Canada's central bank. Its mandate, as defined in the *Bank of Canada Act*, is "to promote the economic and financial welfare of Canada". Receiving data from the OSC on securities and derivatives transactions will enhance the Bank's ability to monitor and assess systemic risks in the financial system. This will enable the Bank to identify potential vulnerabilities and track interconnected exposures thereby supporting its goal of maintaining overall financial stability in Canada.

C. The sharing of the Data with the Bank will avoid duplication of collection, thereby reducing the burden on Canadians and the costs of collecting and processing data.

D. No personal information is being requested by the Bank.

E. The Parties wish to establish in writing the conditions and procedures for the transmission and use of the Data from the OSC to the Bank.

NOW THEREFORE the Parties agree as follows:

1. **DEFINITIONS**

In this Agreement, a capitalized term has the meaning given to it in this section, unless the context indicates otherwise:

"**Data**" means any non-public data and information that is received by the Bank from the OSC through its participation in this Agreement, including without limitation the variables listed in Appendix B.

"**Person**" means an individual, a partnership, a federal, provincial, or municipal entity, a corporation and a not-for-profit organization.

"**Federal Authority**" has the meaning ascribed to such term in section 5.5.

2. **NO REPRESENTATION OR WARRANTY**

No representation or warranty, whether express, implied or otherwise, has been made by the Parties, except as expressly set out in this Agreement. Without limiting the foregoing, the OSC makes no representation or warranty in respect of the accuracy, completeness, quality, title, non-infringement or fitness for a particular purpose of the Data shared under this Agreement and the OSC shall not be liable to the Bank for any losses, costs, damages, expenses or liabilities of any kind or for any claim or cause of action, including negligence, arising out of the provision of the Data.

3. **COLLECTION OF DATA AND AUTHORITY TO SHARE**

3.1 There shall be no requirement for the OSC to collect data or other information that it does not already collect or that it ceases to collect.

3.2 If the OSC becomes aware of a real or suspected error or inaccuracy in its reported Data that would have a material effect on the use of the Data, it will make reasonable efforts to advise the Bank, in writing, of the error or inaccuracy.

3.3 The OSC represents that it has the authority to disclose the Data to the Bank and that such disclosure does not violate any applicable laws.

4. **INFORMATION TO BE SHARED**

The details on the Data to be shared between the Parties are outlined in Appendix B.

5. **CONFIDENTIALITY AND USES OF THE DATA**

5.1 The OSC will transmit the Data to the Bank by secure means of transmission.

5.2 The Bank will ensure that appropriate security measures are taken to protect against loss, theft, corruption or unauthorized access, use or disclosure of the Data, including without limitation, the security requirements set out in Appendix A.

5.3 The Bank will ensure that it has adopted reasonable policies and procedures to protect its own confidential and proprietary information and that, subject to section 5.5 below, it will keep confidential all Data disclosed to it by the OSC, to the extent permitted by applicable law, by using at minimum a standard of care that the Bank would be reasonably expected to employ for its own confidential and proprietary information.

5.4 Without limiting section 5.3, the Bank shall restrict access to the Data to Bank employees , consultants, subcontractors or professional advisors, who (i) need to know the Data for the purposes set forth above; and (ii) are informed of the confidential nature of the Data and agree to treat the Data in accordance with the terms of this Agreement, provided that such disclosure shall be limited to that portion of the Data necessary for the employee, consultant, subcontractor or professional advisor to perform his or her function.

5.5 The Bank may onward share Data that it has obtained under this Agreement by communicating the information orally or in writing to the Department of Finance Canada, the Office of the Superintendent of Financial Institutions, and the Canada Deposit Insurance Corporation (each, a "**Federal Authority**"), provided that the Bank informs the Federal Authority of the confidential nature of the Data and the Federal Authority agrees to not further disclose such information to any person unless:

(a) such disclosure is made to the Cabinet of Canada, in which case prior written consent is not required; or

(b) the Federal Authority first obtains the written consent of the OSC, or in the case where such disclosure is required by applicable law or legal process, promptly notifies the OSC and complies with the provisions of section 5.6.

5.6 In the event that the Bank is required by statute or by legal process (including, without limitation, access to information legislation and a discovery process relating to judicial or administrative proceedings) to disclose Data to a third party, such the Bank will, to the extent permitted by applicable law, promptly notify the OSC, indicate what information it is required to release and the circumstances surrounding its release. If requested by the OSC, the Bank will use its reasonable efforts to preserve its confidentiality to the extent permitted by law, including by asserting all available legal exemptions from or privileges against disclosure.

5.7 Nothing in this Agreement restricts the Bank from informing financial institutions and relevant authorities, or otherwise making public, risks or deficiencies that it has identified when doing so is in connection with its statutory responsibilities or pursuant to legal obligations, even when the knowledge of such risks or deficiencies is based in whole or part on Data, so long as no Data provided by the OSC is disclosed, except in accordance with this Agreement.

5.8 The Bank confirms that it will use the Data only in connection with its statutory responsibilities, mandate, and related activities, including but not limited to policy development, analysis, and general research purposes, unless so authorized in writing by the OSC. The OSC agrees that this may include the preparation and publication of non-commercial research papers, notes, summaries, aggregates, and similar documents using the Data in accordance with section 5.9 of this Agreement.

5.9 The Bank will only release or publish aggregates of the Data that do not directly identify a Person or entity.

5.10 The Bank shall report any loss, theft, unauthorized access, use or disclosure of the Data to the OSC or any cybersecurity attack involving the Data, to the OSC as soon as reasonably possible and in any event within two (2) business days of becoming aware of such incident.

6. **OWNERSHIP OF THE DATA**

6.1 The Data is and shall remain the exclusive property of the OSC and nothing herein grants the Bank any right, title or interest herein.

6.2 Notwithstanding section 6.1, the Bank shall own all rights, title, and interest in and to any derivative works, analyses, reports, papers, or other materials or works created by the Bank as a result of processing or analysing the Data. Such derivative works or materials shall not be considered Data and may be used by the Bank for its own purposes, subject to any confidentiality obligations set forth in this Agreement.

7. **NOTIFICATION OF NON-COMPLIANCE**

A Party shall notify the other Party in writing immediately upon becoming aware that any of the provisions of this Agreement may have been breached. The selected method of communication must allow the Party being notified to receive the notice as soon as possible and in any event within two business days of being sent.

8. **TERM AND WITHDRAWAL**

8.1 This Agreement comes into force on the date that the Agreement is signed by both Parties.

8.2 A Party may at any time withdraw from this Agreement upon giving the other Parties at least ninety days prior written notice. During the notice period, a Party wishing to withdraw from this Agreement will continue to cooperate in accordance with this Agreement.

8.3 The OSC agrees that, after termination of this Agreement, the Bank may retain the Data in perpetuity, provided such Data is maintained in accordance with section 5. For greater certainty, the OSC will not require, upon termination of or withdrawal from this Agreement, the Bank to return or destroy Data received by the Bank as a result of this Agreement.

9. **LIMITATION OF LIABILITY**

The OSC and its members, directors, officers and employees shall not be liable to the Bank for any losses, costs, damages, expenses or liabilities of any kind or for any claim or cause of action, including negligence, arising out of or relating to this Agreement. Without limiting section 10, the Bank shall not be liable to the OSC for any indirect, special, consequential, or punitive damages.

10. **INDEMNIFICATION**

The Bank shall be responsible for and defend the OSC against any third-party claims arising from or relating to (i) the Bank's material breach of this Agreement, (ii) the Bank's gross negligence or wilful misconduct in the use of the Data, or (iii) any unauthorized use or disclosure of the Data by the Bank.

11. **RESPONSIBLE OFFICIALS**

The Parties have designated the Officials listed below as the points of contact for the administration of the provisions of this Agreement.

11.1 The Official for the Bank will be:

Stéphane Lavoie
Managing Director of the Financial Markets Department
Bank of Canada
StephaneLavoie@bank-banque-canada.ca

11.2 The Official for the OSC will be:

Grant Vingoe
Chief Executive Officer
Ontario Securities Commission
20 Queen Street West, 20th Floor
Toronto ON, M5H 3S8
gvingoe@osc.gov.on.ca

12. **DISPUTE RESOLUTION**

Where a dispute arises as to the interpretation of this Agreement or of matters relating to its termination, or of performance hereunder, the Officials for both Parties will attempt in good faith to resolve the dispute through negotiation. Should negotiation prove unsuccessful, the Officials will submit the matter to their senior management for resolution.

13. **NOTICE OF CHANGE**

The Parties undertake to give each other sixty (60) days' notice in writing of any changes in their respective programs, policies or legislation which may affect this Agreement.

14. **AMENDMENT**

No amendment to this Agreement will be effective unless it is made in writing and signed by the Officials, subject to required authorizations.

15. **GENERAL**

15.1 **Entire Agreement**

This Agreement constitutes the entire and only agreement on the disclosure of the Data between the Parties and supersedes all previous negotiations, communications and other agreements, whether written or oral, unless they are incorporated by reference in this Agreement. There are no terms, covenants, representations, statements or conditions binding on the Parties other than those contained in this Agreement.

15.2 **Notices**

Unless otherwise specified in the Agreement, any notice or other communication required to be given or made by either Party shall be in writing and be effective if sent by registered mail, e-mail, postage prepaid or delivered in person, addressed to the respective Party at the contact information outlined under section 11 of this Agreement. Notices shall be deemed to have been given as follows: if by registered mail when the postal receipt is acknowledged by the other Party; if by e-mail on the day of sending, provided no error message is received; if by mail on the eighth (8th) calendar day following the day of mailing; and if by personal delivery on the day of delivery.

15.3 **Law**

This Agreement shall be governed by and construed in accordance with the laws of the Province of Ontario and all applicable laws of Canada.

15.4 **Waiver**

Any tolerance or indulgence demonstrated by one Party to the other, or any partial or limited exercise of rights conferred on a Party, shall not constitute a waiver of rights, unless expressly waived in writing by that Party.

15.5 **Severance**

If any provision of this Agreement, whether in whole or in part, is held by a court of competent jurisdiction to be void or unenforceable, such provision or portion thereof declared invalid or unenforceable shall be deemed to be severable and shall be deleted from this Agreement and all remaining terms and conditions of this Agreement will continue to be valid and enforceable.

15.6 **Survival**

The sections of this Agreement regarding restrictions on use, confidentiality, termination and general, and any other provisions which by their nature survive the termination or expiry of this Agreement, will survive any termination or expiration of this Agreement.

15.7 **Counterparts signature**

This Agreement may be signed in counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument. This Agreement may be executed and delivered in PDF format sent by email transmission. Executed agreements in PDF format sent by email transmission shall have the same legal effect as manual signatures.

This Agreement has been signed by the Parties on the dates indicated below.

FOR BANK OF CANADA:

"Stéphane Lavoie"	Stéphane Lavoie
_____	_____
Stéphane Lavoie, Managing Director, Financial Markets Department	Print Name

DATED at Ottawa, Province of Ontario, this 19th day of February, 2025.
(Month) (Year)

FOR THE ONTARIO SECURITIES COMMISSION:

"Grant Vingoe"	Grant Vingoe
_____	_____
Grant Vingoe, Chief Executive Officer	Print Name

DATED at Toronto, Ontario, this 13th day of February, 2025.
(Month) (Year)

APPENDIX A

SECURITY REQUIREMENTS

Data protection techniques and best practices:

The following data protection techniques and best practices are expected to be followed with respect to the management, use and storage of the Data:

- **Data classification**: The categorization of data based on its sensitivity and importance. Common classifications include public, private, internal use only, confidential and restricted. Classifications such as these, help prioritize security measures and allocate resources appropriately.

- **Data encryption:** The conversion of readable data into an encoded format to protect against unauthorized access. By employing cryptographic algorithms, data encryption protects data from being accessed or deciphered without the corresponding decoding key.

- **Tokenization**: A form of data obfuscation that replaces sensitive data with unique tokens. This is sometimes referred to as data anonymization and pseudonymization. Removing or replacing identifiable information with opaque identifiers can make it difficult for attackers to link sensitive data to an individual.

- **Secure data storage**: Ensures sensitive information — whether it's stored on-premises or in the cloud — is protected from unauthorized access, data breaches and physical theft. Secure data storage measures include techniques such as encryption of data at rest and physical security measures at data centers.

- **Data backup and recovery**: Involves regularly creating copies of essential data and ensuring they can be quickly restored in case of data loss, corruption or system failure. This technique is often grouped with data redundancy measures, which involve creating multiple copies of data for storage in different locations.

- **Data life cycle management**: Includes the processes and policies that guide the creation, storage, usage and disposal of data, ensuring its security and compliance throughout its existence.

- **Access control and authentication**: Restricts access to sensitive data based on user roles, privileges and credentials.

- **Data loss prevention (DLP)**: Includes strategies and tools that detect and prevent the loss, leakage or misuse of data through breaches, exfiltration transmissions and unauthorized use. DLP tools include patching, application control, and device control, which all help protect data by limiting the surface area available to threat actors. Two specific components are worth highlighting:

    - **Endpoint security**: An essential component of DLP focused on defending endpoints — such as desktops, laptops and mobile devices — from malicious activity. By implementing strong endpoint security measures, organizations can prevent unauthorized access and mitigate the risk of data loss through these devices.

    - **Insider risk management**: Monitors and analyzes the behavior of your organization's most trusted users to detect and respond to potential data loss, whether stemming from malicious intent or accidental actions. By implementing an effective insider risk management strategy, you can more easily identify unusual activity and better detect data exfiltration attempts.

- Follow the principle of least privilege.
- Monitor access to sensitive information and user activity.
- Conduct regular security assessments and internal reviews.
- Enforce strong passwords, VPN and multi-factor authentication (MFA).
- Incorporate access removal into your employee offboarding.
- Conduct regular security awareness training.

APPENDIX B

DATA TO BE SHARED

The purpose of the Agreement is to share with the Bank, OTC derivative transaction data collected by the Ontario Securities Commission as part of its mandate as securities regulator in the province of Ontario. This information will be used by the Bank to identify potential vulnerabilities and track interconnected exposures thereby supporting its goal of maintaining overall financial stability in Canada, including the preparation and publication of non-commercial research papers, notes, summaries, aggregates, and similar documents using the Data.

The OSC will provide the following information to the Bank:

Information collected by the OSC on derivative transactions on a trade-by-trade basis including data that describes the economic terms of each position as collected by the OSC and as agreed to by the Bank and the OSC.