NATIONAL BANK

Privacy Booklet

2023

Table of Contents

3 Our One Mission

4 About This Booklet

5 Our Commitment

6 Our Privacy Governance Framework

8 Our Privacy Program

9 Our Privacy Practices

- › Privacy Policy
- › Ethical practices
- › Training and awareness
- › Relationship with our service providers and business partners
- › Automated processing of your personal information
- › Collection and use of your digital data through cookies and other similar technologies
- › Complaint and incident management
- › Cross-border data movements
- › Life cycle of personal information

15 Our Performance in 2023

15 Questions or Comments?

OUR ONE MISSION

We exist to have a **POSITIVE IMPACT** in people's lives.

By building ***long-term relationships*** with our clients, employees and communities.

People first.

Why do we need a One Mission?

Our One Mission is aligned with our continued efforts to drive social and economic development. In response to changing trends in the banking industry, we've adopted a people-first approach that will help us achieve our objectives and boost our collaboration with stakeholders.

How is our One Mission put into practice?

- Through the experiences we want to deliver to our clients, our employees and the communities we serve.
- Through behaviours that reflect our values: partnership, empowerment and agility.
- Through the way employees work together to boost client satisfaction, employee engagement and community involvement.
- Through the initiatives we prioritize to have a positive impact.

About This Booklet

This booklet on privacy is produced by National Bank of Canada's Privacy Office. It is a testament to our commitment to being transparent and offering you an experience in line with your expectations.

Privacy is one of the Bank's priorities. Over the years, measures have been put in place to reinforce our practices and earn your trust. These practices are set out in this booklet. We will keep you informed of any related progress and results on an annual basis.

Scope

The information in this booklet covers the activities of the Bank and its main Canadian subsidiaries[1] for the period from November 1, 2022, to October 31, 2023.

Who it is for: stakeholders

This booklet has been prepared to help our stakeholders understand our privacy program. It reflects a summary of our program as well as our privacy practices, policies and standards and our voluntary disclosure efforts. This booklet aims to foster an ongoing dialogue between the Bank (including its directors and officers) and its clients, employees, shareholders and service providers as well as communities, interest groups and regulatory authorities. This dialogue helps us enrich our practices and aim for the most advanced privacy and disclosure standards.

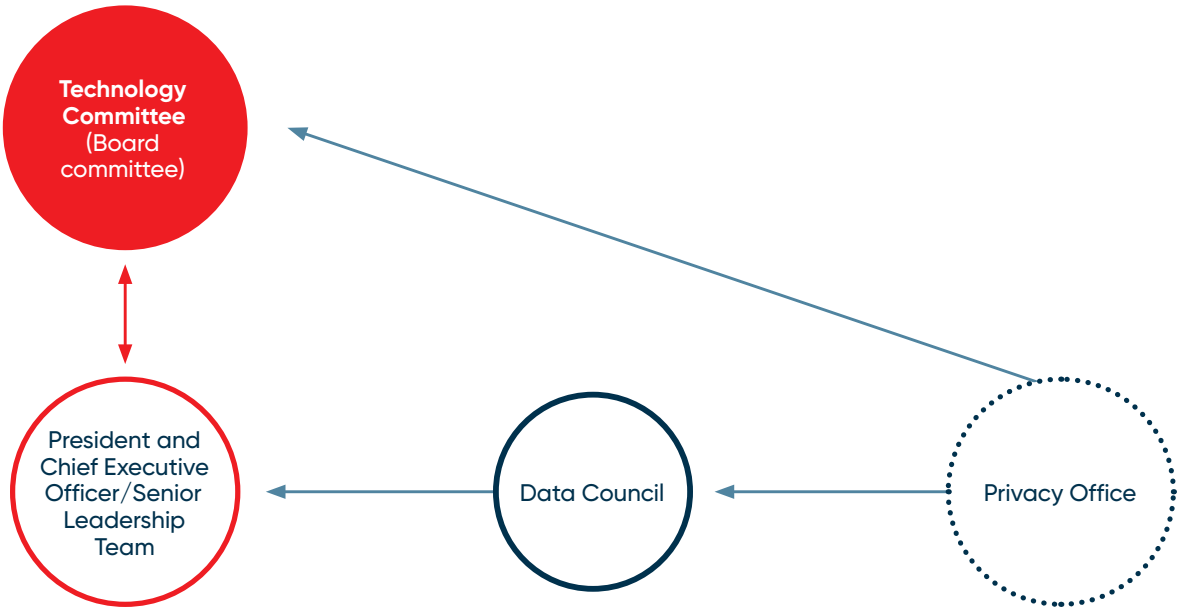
1 The information provided in this report does not include Flinks Technology Inc.

Our Commitment

> We do our utmost to ensure the protection of your personal information. All of our employees work together towards this goal.
>
> Our commitment to you is simple: to maintain a relationship of trust.

Our commitment is aligned with the Governance component of our Environmental, Social and Governance (ESG) principles, which have been approved by the Bank's Board of Directors. Our commitment to privacy advances the United Nations (UN) Sustainable Development Goals, and goal 16 in particular: Peace, Justice and Strong Institutions. We have put in place a governance framework for the protection of personal information to ensure that we protect your information and maintain a relationship of trust with you.

Our Privacy Governance Framework



Privacy Office

The Privacy Office is headed by the Chief Privacy Officer, who reports to the Senior Vice-President, Legal Affairs and Corporate Secretary of the Bank.

The Office develops and implements our privacy program and privacy strategy; its responsibilities include oversight related to:

- developing, updating and implementing relevant documents in support of our privacy program, such as our policies, standards and procedures;
- the privacy risk governance framework; and
- establishing appropriate controls for risk mitigation.

The Office's responsibilities also include:

- ensuring the reliable protection and processing of personal information as well as compliance with applicable laws;
- supporting the Bank's business sectors in carrying out the adopted strategic orientations;
- proactively monitoring any new legislative requirements regarding the protection of personal information and ensuring compliance with best practices;
- analyzing emerging issues that may affect our internal practices and our commitments to you;
- making recommendations to various decision-making levels; and
- participating in the socialization of various privacy reform initiatives.

The Privacy Office periodically presents the various committees with:

- reports on privacy risks and the status of strategic initiatives; and
- new facts as well as emerging trends that may impact current practices.

The Board of Directors and the Technology Committee

The Bank's **Board of Directors**, through **the Technology Committee**, ensures that the Bank's technology strategy is implemented and that the oversight and management of technology risks, including cyber risks, cybercrime and the protection of personal information, are properly applied and carried out. The roles and responsibilities of the Board of Directors and the technology committee are described more fully in their respective mandates. Their respective mandates as well as their main achievements (available in the Bank's most recent management proxy circular) can be respectively consulted in the subsections of the nbc.ca website devoted to governance and investors, under the tab "About Us".

The Data Council

The **Data Council** is composed of the Bank's executives and is interested in how the Bank manages data, including personal information, with a mandate to set the Bank's strategic orientations. At its monthly meetings, the Council is required to approve initiatives involving personal information that could have a significant impact on the orientations adopted by the Bank. The Data Council is supported by committees that assist in data risk oversight. For example, the Data Risk Committee oversees the integration of data risks, including privacy risks, into the risk management processes across various sectors.

The Executive Officers

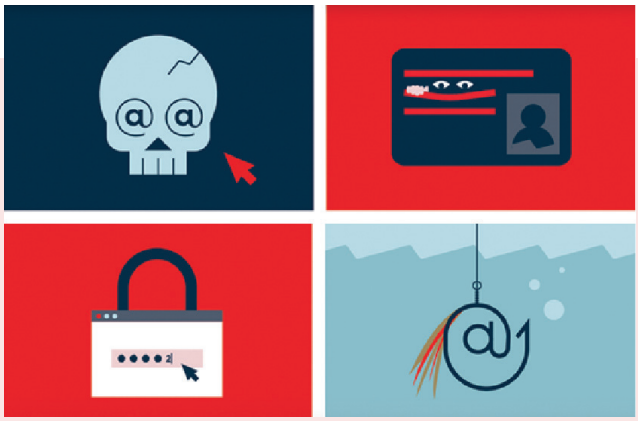
The President and Chief Executive Officer as well as the Senior Leadership Team approve the main strategic orientations and priorities relating to the protection of personal information. They are ambassadors within the organization and to the Bank's Board of Directors with regard to the protection of personal information.

Strengthening our governance through privacy champions

As an institution, we are committed to creating a culture dedicated to protecting your personal information, one that resonates across all functions in our organization. In order to strengthen our governance, we have appointed "privacy champions" who support the Bank's initiatives involving personal information to leverage privacy in business strategies. They are, in a manner of speaking, the eyes and ears of the Privacy Office on the ground.

The role of the privacy champion is to:

- support business sectors with the development and implementation of projects, processes and control to ensure sound management of personal information;
- identify business issues as well as any awareness and training needs for the business sectors they support; and
- support business sectors assessing privacy-related risks.

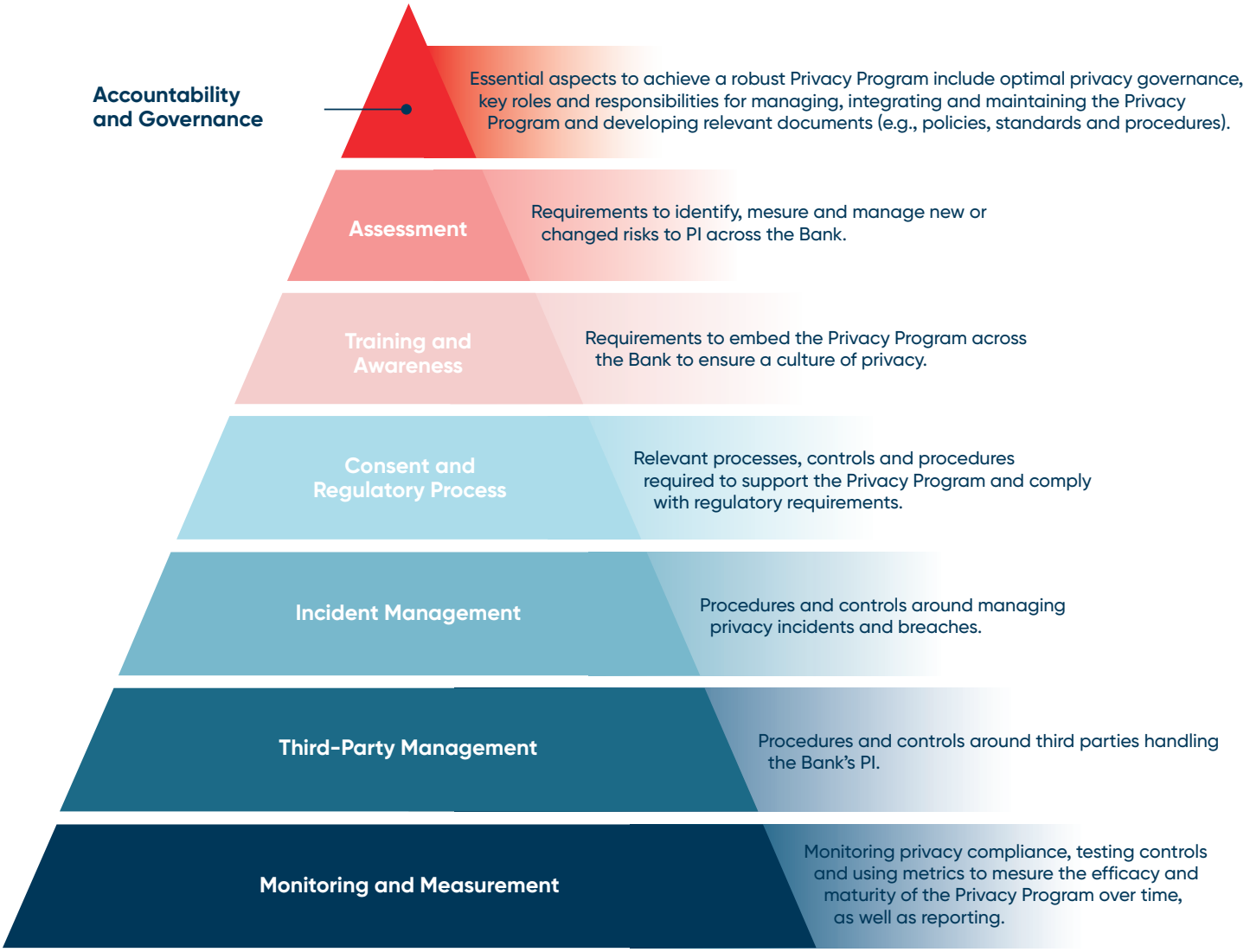


Protecting personal information, a shared responsibility

The protection of personal information is the result of the collaboration and combined efforts of several business sectors and internal committees. Our personal information governance involves a **reporting process**. This process enables us to gauge the effectiveness of our practices so we can make decisions based on our commitment to you, our risk appetite and our ambition to offer you innovative products and solutions.

Our Privacy Program

The protection of individuals' personal information is crucial to accelerate our business model and strategies. Indeed, compliance with the various privacy requirements as well as managing and safeguarding personal information appropriately are the basis of the relationship of trust with all our stakeholders. Proper management of personal information preserves and increases this relationship of trust, creates value for our clients and for our organization and reduces the risks associated with the processing of personal information. Our privacy program, which enables us to achieve these goals, is based on the following seven pillars:



Our Privacy Practices

We oversee the protection of your personal information as follows:

- With a **privacy policy**, in which the Bank sets out the responsible practices it has adopted for the collection, use and disclosure of your personal information.
- With a **digital data policy**, the goal of which is to be transparent about our use of technologies allowing us, with your permission, to collect and use certain data from your device and browsing habits.
- Through effective **internal controls** to detect and prevent confidentiality incidents throughout the entire life cycle of personal information.
- Through **continuous risk assessment: several privacy-related activities are in place to identify, assess and manage risks**, whether they are new or created as a result of technological changes, procedures or business initiatives.
- Through **management of access and correction requests, complaints and incidents**.
- By providing **training** to all our employees.

Privacy Policy

We have developed **our privacy policy** with you in mind. Your consent is the cornerstone of our practices: we respect your choices and act based on the consent you have given.

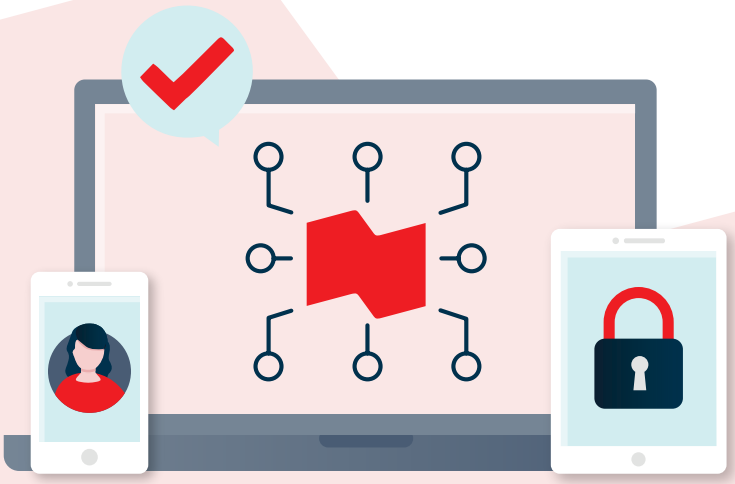
This policy explains, among other things:

- what types of personal information we may collect and from whom;
- how we can use and share your information and with whom;
- the choice you have in consenting or not to certain uses of personal information; and
- our approach to retaining and destroying your personal information.

The policy also informs you about your rights to:

- access and consult the personal information we have about you;
- correct your personal information to ensure its accuracy;
- opt out of receiving our product and service offers and other promotional communications at any time; and
- refuse that we collect and use your digital information on our online services.

When you enroll in new products or services, we will notify you of any significant changes to our policy through our digital channels and telephone banking services or via any other appropriate means.



Ethical practices

Technological transformations, especially those related to artificial intelligence and advanced analytics technologies, are drawing more and more attention. As an organization, we are mindful of the effects that these technologies can have on rights and freedoms as well as on our ability to positively transform the experience of our clients and employees. We therefore proactively assess our practices to make sure that the technologies we deploy are aligned with our values.

For example, our program that focuses on fairness by design enables us to strengthen our artificial intelligence and advanced analytics activities. This cross-sector program provides for concrete measures that help reinforce equity best practices and awareness and training activities for business development teams and data science teams alike.

This program includes concrete measures implemented in development teams and supervision teams. In this context, awareness and training activities were held within the different sectors of the Bank, both for business development and scientific teams as well as for employees of the second and third lines of defense. Performance indicators are in place to monitor our equity practices. For example, we track the effective adoption rate of the program by the analytical solutions that we have put into production in the last year. **As of October 31, 2023, this adoption rate is 100%, with a target of 90%**.

> Under no circumstances do we sell client lists to third parties.

Training and awareness

Our approach is as follows:

1. Mandatory training for new employees that makes them aware of the importance of privacy for the Bank and our clients, and equips them with the tools to protect this information.
2. Continuously raising awareness through training modules and activities to keep employees informed.
3. Targeted training to support certain business sectors—for example, when deploying a new initiative or improving processes.

Our goal is to have **dedicated employees who are aware** of the importance of protecting your personal information. Training is offered at all levels of our organization.

Training is updated periodically to meet new regulatory requirements and best practices. Our Code of Conduct also reinforces the importance of protecting personal information.

Annual mandatory training: privacy governance Framework – The actions we take to maintain our clients' trust

In 2023, we deployed a new mandatory training on our privacy governance framework and the roles and responsibilities of employes regarding the protection of personal information.

96 % of active employees successfully completed the training.

In 2022, the training regarding our commitment to preserving trust was successfully completed by 91% of active employees.

Annual regulatory compliance training

The annual regulatory compliance training contains a specific segment on destruction practices and access management of personal information.

Training on individual rights

In 2023, employees who work directly with customers and the specialized teams who support them received training on individuals' rights regarding the protection of their personal information. These rights include access to personal information, the correction of inaccurate or incomplete personal information and the filing of a privacy complaint. This training allowed employees to increase their understanding of these rights and to learn how to respond effectively to such requests by following the procedures in place.

Relationship with our service providers and business partners

The safety of your personal information is important, including when it must be sent to third parties. We take great care in choosing our business partners and service providers. We have a third-party risk-management procurement process. When it is necessary to use a service provider or a business partner who will hold information (including personal information) for which we are responsible, our process is applied and the elements related to the protection of personal information are integrated in all stages of the life cycle of a service provider or business partner.

The life cycle of a service provider or business partner

- **Materiality Assessment:** We perform a materiality assessment that includes privacy risk-related questions.
- **Due-Diligence Review:** We initiate a due-diligence process that includes a security and privacy due diligence review.
- **Negotiation of Agreements:** Our service providers or business partners may only use personal information in a responsible and ethical manner. They agree to use only the personal information required to provide their service and must be as diligent and cautious as we are to ensure the security of your personal information.
- **Agreement Management:** We ensure the right oversight mechanisms are in place to monitor, among other things, compliance with security and privacy requirements. We also require that our service providers and business partners notify us of any privacy incidents so that we can work together to respond, remedy and, if applicable, report them.
- **Renewal, Expiry or Termination of Agreements:** If we decide not to renew the agreement with our service provider or business partner, the Bank and its service provider or business partner follow the relevant contractual clauses, in particular those relating to the retrieval and the destruction of personal information.

Automated processing of your personal information

In the interest of being transparent with you, when we use your personal information to make automated decisions about you, for example, in response to your requests for certain credit and financing products, we will inform you of such decisions, at the latest, when they are communicated to you. A decision is automated when, as a rule, no human is significantly involved in the decision-making process.

At any time, you can contact us to find out the personal information that was used to make the decision and the main reasons leading to the decision. You also have the right to have inaccurate information that was used to make the decision corrected. The fair and equitable treatment of your personal information as part of our automated decision-making processes is at the heart of our priorities.

Collection and use of your digital data through cookies and other similar technologies

We have deployed a banner on our websites and our National Bank mobile application that appears during your first visit. This banner gives you the choice to allow or refuse optional technologies that collect and use your digital data, such as certain information about your device and your browsing habits. You will have access to our websites and our mobile application, regardless of your preferences. To learn more, you can consult our Digital Data Policy.

Complaint and incident management

Complaint management

The Bank wants to be transparent about how it manages your personal information, in addition to ensuring that your personal information is treated in a sound and reasonable manner. Your complaints and dissatisfactions relating to the protection of personal information are taken very seriously. In order to quickly find solutions that suit you, the Bank has recently strengthened its complaint-handling processes relating to the protection of personal information and trained its employees to enable them to manage this type of complaint according to the procedures in place.

Our employees and Privacy Office work together to answer your questions about the protection of your personal information, to guide you and to find solutions that are right for you.

> You have several simple options to communicate your concerns and complaints to us.

For a question or comment, you can contact:

- the customer service manager of your branch,
- your investment advisor or representative, or
- our Chief Privacy Officer or by writing to us at confidentiality@nbc.ca

To make a complaint, you must follow the procedures outlined on our website at **nbc.ca**, under About us > Useful links > Complaint settlement online.

Confidentiality incident management that may involve personal information

We make significant efforts to protect your personal information from loss, theft and unauthorized access, use or disclosure. We have practices in place that allow us to identify and fully understand our risks. We have a security program in place to keep pace with changing information security threats. The measures adopted in our security program include:

- protecting the infrastructure through secure access to our premises and secure locations for our equipment, etc.
- limiting who has access to your information. This means that only employees who need to know your information in order to carry out their duties have access to it; and
- managing passwords and setting up firewalls.

If an incident that presents a real risk of serious injury to your information should occur, you will be personally informed within the time limits provided by law.

Cross-border data movements

If it is necessary to move data across borders as part of our activities, we make sure to comply with applicable laws and the best practices in this area. Risk assessments are carried out taking into consideration the various legal and regulatory requirements, the legal and socio-political context of the recipient countries, and the volume and sensitivity of the information shared, all in order to ensure that a comparable degree of protection to the country of origin can be offered. Four principles must be followed before proceeding with a cross-border movement of data: necessity, knowledge, evaluation and governance.

Life cycle of personal information

Life cycle of personal information

- **Collection:** We limit the collection of your information to what is necessary to help us serve you properly.
- **Use:** We use your information in accordance with our Privacy Policy and our Digital Data Policy.
- **Communication:** At all times, we are committed to limiting the information to what is necessary.
- **Retention:** We retain your information for as long as necessary to fulfill the purposes for which the information was collected or as long as required or permitted by law. Our legal obligations, the purpose for collecting the information as well as the nature and the sensitivity of the information have been considered in determining retention periods. We have reviewed and simplified our retention periods to clarify the triggering event of the retention period.
- **Destruction:** When your information is no longer needed, we endeavour to securely destroy it.

For more information about our practices, please see our Privacy Policy.

Our Performance in 2023

Our practices are evolving, and we are continuously improving our performance indicators to better assess the quality of our practices. Our goal is to improve the effectiveness of our strategies and operational processes.

We have implemented an indicator based on the number of decisions made annually by regulators regarding the Bank.

Decisions regarding personal information involving the Bank	Annual target	Result in 2023
	0	0

Questions or Comments?

Your feedback is important to us. We are committed to following up on it in a straightforward manner so you can understand how we handle your personal information.

If you have any questions or comments, please contact:

1. **Your branch's Customer Service Manager**

2. **The Chief Privacy Officer** at:
   confidentiality@nbc.ca
   or
   600 De La Gauchetière Street West, 4th Floor
   Montreal, Quebec, Canada H3B 4L2

NATIONAL BANK

31959-002 (2023/01)