

# Scotiabank Code of Conduct



## A message from our CEO

- Introduction

---

- Our guiding principles

---

- Principle 1

---

- Principle 2

---

- Principle 3

---

- Principle 4

---

- Principle 5

---

- Principle 6

---

- Getting help or reporting problems and irregularities

---

- Glossary

---

- Key sources of guidance and advice



Since welcoming our first customers in 1832, Scotiabank’s reputation has been the foundation of our business. The choices and decisions we make daily underpin the confidence that customers, employees, shareholders and communities have in our organization, and the strong relationships we have been able to build and maintain with them.

Our reputation is something we must never take for granted. We must all strive to protect and strengthen it, if we are to maintain our position as Canada’s most international bank.

Our values, including acting with respect, passion, integrity and accountability in everything we do, are essential to maintaining our good name and demonstrating our belief that every customer has the right to become better off. Meeting sales goals or profitability targets is important, but absolutely nothing is more important than staying true to our values – even when it is difficult, or seems to conflict with other priorities.

From time to time, all of us face tough decisions, when we may be uncertain about what we should or shouldn’t do or say. To help you in these difficult situations, we have set out the basic standards of ethical behaviour that each of us is required to follow in the *Scotiabank Code of Conduct*. We have included examples of common questions and problematic situations, and what you should do when these occur.

Without question, conduct reflects culture. While we have much to be proud of in this regard at Scotiabank, building and maintaining the right culture requires constant attention. Please read this Code carefully, think about what it means to your own job and workplace situation, and use good judgment to apply the principles every day in your actions at work. It’s not possible for this Code to cover every situation, so if you aren’t sure about the right thing to do, consult your Manager or a more senior officer. Consult the *Pathways to Resolution* guide – or any of the other options described in this Code – to let management know about any questions or issues you encounter. Complying with the requirements and principles of this Code is a condition of your employment and, every year, you will be asked to affirm that you have read, understood and followed this Code.

By living up to the principles set out in this Code, and working together to sustain our core values, we can build upon our culture of integrity and entrust future generations of Scotiabankers with the gift of the enviable reputation we have inherited.

Sincerely,

Brian J. Porter  
President & Chief Executive Officer

# Table of contents

- Introduction

---

- Our guiding principles

---

- Principle 1

---

- Principle 2

---

- Principle 3

---

- Principle 4

---

- Principle 5

---

- Principle 6

---

- Getting help or reporting problems and irregularities

---

- Glossary

---

- Key sources of guidance and advice

**Introduction**

- I. Roles and responsibilities . . . . . 4
- II. Consequences of failing to comply with the code . . . 5
- III. Scotiabank policies . . . . . 5
- Our guiding principles . . . . . 6



**Principle 1**  
**Follow the law wherever Scotiabank does business**

- I. Your responsibilities . . . . . 7
- II. Conflicting requirements . . . . . 7



**Principle 2**  
**Avoid putting yourself or Scotiabank in a conflict of interest**

- I. Personal conflicts of interest . . . . . 8
- II. Corporate conflicts of interest . . . . . 12



**Principle 3**  
**Conduct yourself honestly and with integrity**

- I. Illegal or fraudulent activities . . . . . 13
- II. Improper transaction prevention . . . 15
- III. Ethical business practices . . . . . 16
- IV. Engaging third parties . . . . . 18
- V. Communications and representations . . . . . 18
- VI. Cooperate with audits and investigations . . . . . 19



**Principle 4**  
**Respect confidentiality, and protect the integrity and security of assets, communications, information and transactions**

- I. Privacy and confidentiality . . . . . 20
- II. Accuracy and integrity of transactions and records . . . . . 21
- III. Security . . . . . 22
- IV. Digital communications, use and representation . . . . . 23



**Principle 5**  
**Treat everyone fairly, equitably and professionally**

- I. Diversity, equity and human rights . 24
- II. Workplace health and safety . . . . . 24



**Principle 6**  
**Honour our commitments to the communities in which we operate**

- I. Environmental protection . . . . . 25
- II. Charitable and community activities . . . . . 25
- III. Political activities . . . . . 25
- IV. Other codes of conduct and voluntary commitments . . . . . 25

**Getting help or reporting problems and irregularities**

- I. Obligation to report . . . . . 26
- II. Protection from retaliation . . . . . 26
- III. How to report . . . . . 27

**Glossary . . . . . 28**

**Key sources of guidance and advice . . . . . 30**

# Introduction

► Introduction

- I. Roles and responsibilities
- II. Consequences of failing to comply with the code
- III. Scotiabank policies

Our guiding principles

Principle 1

Principle 2

Principle 3

Principle 4

Principle 5

Principle 6

Getting help or reporting problems and irregularities

Glossary

Key sources of guidance and advice

The *Scotiabank Code of Conduct*<sup>1</sup> (the “Code”) describes the standards of conduct required of employees, directors and officers of The Bank of Nova Scotia and its direct and indirect subsidiaries located in various regions around the world (“Scotiabank” or the “Bank”).

If you are uncertain about what is the most appropriate course of action in a particular situation, this Code should be your first point of reference. If there is something in this Code that you don’t understand, or if you require additional guidance, ask your Manager or a more senior officer.

Consult the glossary at the end of this document for definitions of some of the key terms used in this Code.

1 This version of the Scotiabank Code of Conduct was approved by the Board of Directors on August 30, 2016. The online version of this Code, available at [www.scotiabank.com](http://www.scotiabank.com), is the most up-to-date, and supersedes prior versions.

2 Notwithstanding the Board of Directors’ authority over changes and waivers of this Code, Enterprise Programs Compliance has the discretion to authorize: (1) the waiver of particular provisions which clearly conflict with local laws; and (2) non-substantive changes (e.g. for clarification or editorial purposes, to reflect new regulatory requirements or changes to terminology or to ensure that cross-references to other Scotiabank policies are accurate and up-to-date).

3 In certain limited situations, Scotiabank may waive application of a provision of this Code to an employee, director, or officer. The Board of Directors or a Committee of the Board of Directors must approve any waivers involving a director or executive officer of Scotiabank, and any such waivers will be disclosed in accordance with applicable regulatory requirements. All other waivers or exceptions must be approved by appropriate authorities within Scotiabank’s Legal, Compliance and Human Resource Departments. Waivers will be granted rarely, if ever.

## I. Roles and responsibilities

New employees, directors, and officers are given a copy of this Code when they are hired or elected and must acknowledge that they have received and read it. All Scotiabankers are required to receive, read and comply with this Code, and any other applicable Scotiabank policies, affirm their compliance on an annual basis, ask questions when unclear about their responsibilities or the appropriateness of a particular action, and report any actual or potential breach of this Code immediately.

In addition, managers have additional responsibilities to be aware of and communicate applicable laws, regulatory requirements and internal policies, procedures, processes, manage and supervise employees to ensure that the law, regulatory requirements, this Code and other internal policies, procedures and processes are followed. Managers must also respond

to questions from employees, and ensure that any actual or potential breach of this Code is dealt with or escalated in accordance with applicable policies, procedures, and processes.

Executive Management and the Board of Directors have further additional responsibilities. The President & Chief Executive Officer of Scotiabank bears overall responsibility for ensuring that this Code is followed throughout the organization, and reports on compliance with this Code every year to the Board of Directors or one of its Committees. The Board of Directors is responsible for reviewing and approving the content of this Code and must authorize changes<sup>2</sup> to this Code and certain kinds of waivers<sup>3</sup>.

These roles and responsibilities are summarized in the following chart.

Responsibility	Employee	Director	Officer	Manager	Executive Management	Board
Read, understand and comply with code and policies	●	●	●	●	●	●
Affirm compliance	●	●	●	●	●	●
Ask questions	●	●	●	●	●	●
Report breaches	●	●	●	●	●	●
Communicate requirements				●	●	
Supervise compliance				●	●	
Answer questions				●	●	
Address breaches				●	●	
Report on compliance					●	
Approve changes to code					●	●
Approve waivers					●	●

# Introduction

## ► Introduction

- I. Roles and responsibilities
- II. Consequences of failing to comply with the code
- III. Scotiabank policies

### Our guiding principles

#### Principle 1

#### Principle 2

#### Principle 3

#### Principle 4

#### Principle 5

#### Principle 6

### Getting help or reporting problems and irregularities

### Glossary

### Key sources of guidance and advice

## II. Consequences of failing to comply with the code

Unethical or illegal conduct puts Scotiabank, and in some cases its customers, shareholders, employees and other stakeholders, at risk.

For example:

- Scotiabank and/or an employee could be subject to criminal or regulatory sanction, loss of license, lawsuits or fines.
- Negative publicity from a breach of this Code could affect our customers' or potential customers' confidence in Scotiabank, and their willingness to do business with us.

Adherence to both the letter and the spirit of this Code is therefore a condition of employment at Scotiabank.

Any breach, or willful ignorance of the breaches of others, will be treated as a serious matter, and may result in discipline up to and including termination of your employment. Scotiabank may also be required to report certain types of breaches to law enforcement or regulatory authorities, in which case a breach or willful ignorance of the breaches of others may result in your being subject to criminal or civil penalties.

## III. Scotiabank policies

You are expected to be aware of and comply with all other applicable Scotiabank policies, including the following which are specifically identified in this Code:

- *Anti-Corruption Policy;*
- *Corporate Directorships Policy;*
- *Scotiabank Employee Personal Trading Policy and Trade Window Policy;*
- *Human Rights Policy;*
- *Scotiabank Information Security Policy;*
- *Personal Information Privacy Protection Policy and Guidelines;*
- *Reputational Risk Policy;*
- *Statement of Disclosure Policy and Practices and Mandate of the Disclosure Committee;*
- *Scotiabank Expense Policies*
- *Travel Policy;* and
- *Whistleblower Policy and Procedures ("Whistleblower Policy").*

The *Internet and Electronic Mail Code of Conduct* and *Social Media Policy* are no longer stand alone policies but are embedded within this Code.

You should also be familiar with the Code addendum, *Key sources of guidance and advice*. In addition, some countries, subsidiaries or specialized areas may have other supplemental guidelines or codes of conduct that apply to their employees. If you work in one or more of these countries or for one of these subsidiaries or specialized areas, you will be advised of the supplemental guidelines that apply to you and you may be required to acknowledge them annually in the same manner as this Code.

In the case of any conflict between the provisions of this Code and any laws, regulatory requirements or any other policies, procedures, guidelines applicable to your employment duties, you must adhere to the more stringent requirement to the extent the conflict exists.

## Our guiding principles

Introduction

► Our guiding principles

Principle 1

Principle 2

Principle 3

Principle 4

Principle 5

Principle 6

Getting help or reporting problems and irregularities

Glossary

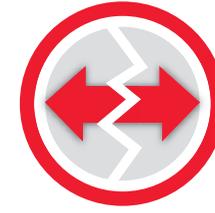
Key sources of guidance and advice

Scotiabank's six guiding principles are aligned with our values and form the building blocks on which this Code rests. Living up to them is an essential part of meeting our corporate goals, adhering to our values, and safeguarding Scotiabank's reputation for integrity and ethical business practices.

The six principles are:



**1** Follow the law wherever Scotiabank does business.



**2** Avoid putting yourself or Scotiabank in a conflict of interest position.



**3** Conduct yourself honestly and with integrity.



**4** Respect confidentiality, and protect the integrity and security of assets, communications, information and transactions.



**5** Treat everyone fairly, equitably and professionally, whether they are customers, suppliers or service providers, employees, or others who deal with us.



**6** Honour our commitments to the communities in which we operate.

### REMEMBER:

Always perform your duties honestly, in good faith, and in the best interests of Scotiabank, its reputation and its customers by exercising the integrity, care, diligence and skill that would be expected of a reasonably prudent person in similar circumstances.

[Introduction](#)[Our guiding principles](#)**▶ Principle 1****Follow the law wherever Scotiabank does business.**

- I. Your responsibilities
- II. Conflicting requirements

[Principle 2](#)[Principle 3](#)[Principle 4](#)[Principle 5](#)[Principle 6](#)[Getting help or reporting problems and irregularities](#)[Glossary](#)[Key sources of guidance and advice](#)**I. Your responsibilities**

Ask questions...comply...report!

There are many forms of law, and Scotiabank and its employees world-wide are expected to comply with the laws that govern their activities. There are legal requirements and regulatory requirements in each of the countries in which we operate. Scotiabank must follow these laws – both the letter and the spirit – wherever it does business, and so must you.

There are also internal Scotiabank policies and procedures, which have been authorized by the Board of Directors or senior management of the Bank or its subsidiaries, that reflect how Scotiabank manages its business strategy and risk appetite. Scotiabankers are expected to know the policies and procedures that are relevant to their activities, act in accordance with the letter and spirit of these policies and procedures, and comply with them. Sometimes policies and procedures may seem cumbersome, but remember that they have been developed with legal, regulatory, business, and/or risk management considerations in mind.

If you are unclear about legal, regulatory or other requirements, consult your Manager. If necessary, he or she can seek the advice of the [Legal Department](#) or [Compliance Department](#).

Be careful to always act within the scope of your assigned authority. Skipping a step, even one that seems redundant, could put Scotiabank, you, your fellow employees, customers, shareholders or others at significant risk.

**Advice that can put Scotiabank at risk**

You are expected to inform customers about Scotiabank products and services. However, do not give specific financial, trust, tax, investment or legal advice unless it is part of your job responsibilities, you hold the appropriate qualifications and licenses and all applicable regulatory requirements are met.

The act of giving advice to a customer can create greater than normal legal obligations, and put you and Scotiabank at risk. Refer customers who request advisory services to their own advisors, or to those employees, areas, or subsidiaries that are authorized to do this type of business with customers.

Immediately report any actual, suspected or potential violations of law, regulations, or internal policies (including instances where you see a risk that appears to have been overlooked or ignored by others) through one of the options described in the [Pathways to Resolution](#) guide (or, where appropriate, under the [Whistleblower Policy](#)), or using the other avenues described in [Getting help and reporting problems and irregularities](#).

In some jurisdictions, Scotiabank is subject to regulation with respect to the sale of insurance, so be sure to follow any instructions applicable to insurance products carefully. You should not recommend that customers use a particular insurance company or agent, or give specific advice on types of coverage for non-Scotiabank sponsored insurance products unless:

- this is permitted by law in your jurisdiction; and
- it is part of your job responsibilities and you hold the appropriate qualifications and licenses.

**II. Conflicting requirements**

If you encounter a situation where this Code or other Scotiabank policies appear to conflict with local cultural traditions, business practices or legal requirements of the country in which you are located, the senior officer involved must consult with the Compliance Department. Keep a written record of such enquiries and responses.



PRINCIPLE 2 | **Avoid putting yourself or Scotiabank in a conflict of interest position**

- Introduction

---

- Our guiding principles

---

- Principle 1

---

- ▶ Principle 2
  - Avoid putting yourself or Scotiabank in a conflict of interest position
  - I. Personal conflicts of interest
  - II. Corporate conflicts of interest

---

- Principle 3

---

- Principle 4

---

- Principle 5

---

- Principle 6

---

- Getting help or reporting problems and irregularities

---

- Glossary

---

- Key sources of guidance and advice

**I. Personal conflicts of interest**

Employees, directors, and officers have an obligation to act in the best interests of Scotiabank. A conflict of interest can arise when there is a conflict between what is in your personal interest (financial or otherwise) and what is in the best interest of Scotiabank or a customer.

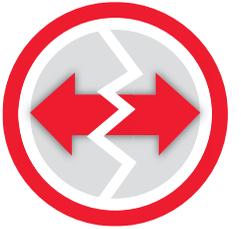
Even if you do not have an actual conflict of interest, if other people perceive one, they may still be concerned that you cannot act properly. For this reason, it is important to avoid the appearance of a conflict, as well as an actual one. Being seen or thought to be in a conflict of interest can damage your reputation, and the reputation of Scotiabank.

If you find yourself in a conflict of interest position or a situation where you believe that others perceive you to be in a position of conflict, you must immediately advise your Manager so that action can be taken to resolve the situation. This is the best way to protect yourself and your reputation for honesty, fairness and objectivity.

Your Manager, who may consult a more senior Manager or the Compliance Department if necessary, will decide if a conflict exists or if there is the potential for the

appearance of a conflict that could be damaging to Scotiabank’s reputation, as outlined in the *Reputational Risk Policy*.

The sections that follow describe some common conflicts that sometimes arise and provide advice on what to do if you encounter any of these situations.



**Sample potential personal conflicts of interest**

Situation	Conflict
A customer names an employee as a beneficiary of his or her will.	The customer’s family, or others, may perceive that the employee used his or her position to unfairly coerce, manipulate or take advantage of the customer.
An employee accepts a gift of tickets for him- or herself and family to an expensive, sold-out sports event from a commercial banking customer.	The employee risks a perception by others that he or she could be improperly influenced in his or her judgment when making lending or other decisions related to the customer’s business accounts at Scotiabank.
An employee accepts a gift from a supplier or service provider who is bidding on a contract to supply services to Scotiabank.	Other suppliers may perceive that either Scotiabank or the employee was influenced by the gift to award the contract to the supplier or service provider.

Introduction

Our guiding principles

Principle 1

## ▶ Principle 2

**Avoid putting yourself or Scotiabank in a conflict of interest position**

- I. Personal conflicts of interest
- II. Corporate conflicts of interest

Principle 3

Principle 4

Principle 5

Principle 6

Getting help or reporting problems and irregularities

Glossary

Key sources of guidance and advice

### a. Transactions that involve yourself, family members or close associates

When you deal with Scotiabank as a customer, your accounts must be established, and your personal transactions and account activities conducted, in the same manner as those of any non-employee customer.<sup>4</sup> This means that you may only transact business, make entries or access information on your own accounts using the same systems and facilities available to non-employee customers. (For example, you can use online banking to transfer funds between your own accounts, since this service is generally available to non-employee customers).

The accounts, transactions and other account activities of your family members, friends and other close associates must also be established and conducted in the same manner as those of other customers. Do not set up accounts on your own behalf, or on behalf of these individuals, without the review and agreement of your Manager. Also, only transact business or make entries or enquiries on accounts of family members, friends or close associates with appropriate authorization from the customer (e.g. in the normal course of business as permitted under a relevant customer agreement, or as authorized by a written trading authority on file).

Under no circumstances may you authorize or renew a loan, or lending or margin limit increase to yourself, a family member, a friend or other close associate. Nor may you waive fees, reverse charges or confer any benefit or non-standard pricing or access Customer Information System (CIS) profiles with respect to your own accounts or those of family, friends or other close associates without the prior review and agreement of your Manager.

### b. Objectivity

Do not let your own interests or personal relationships affect your ability to make the right business decisions. Family members, friends and other close associates should have no influence on your work-related actions or decisions. Make decisions about meeting a customer's needs, engaging a supplier or service provider, or hiring an individual on a strictly business basis.

### c. Outside business activities, financial interests or employment

Employment outside of Scotiabank working hours is permitted if there is no conflict of interest and if the satisfactory performance of your job functions with Scotiabank is not prejudiced or negatively impacted in any way.

In addition, the following rules apply:

- You must not engage in a business that competes with Scotiabank, or in any activity likely to compromise or potentially harm Scotiabank's position or reputation.
- You must not conduct outside business on Scotiabank time, or use Scotiabank equipment or facilities to conduct an outside business interest. This includes soliciting other employees or Scotiabank customers to participate in an outside business activity.
- You owe a duty to Scotiabank to advance its legitimate interests when the opportunity to do so arises. You may not take for yourself a business opportunity that is discovered in the course of your Scotiabank employment, or through the use of Scotiabank property, information (including customer information) or your position.
- Neither you nor members of your household should have a financial interest in, or with, a customer, supplier or service provider of Scotiabank, or any other entity having a close business relationship with Scotiabank, if this would put you in a conflict of interest.<sup>5</sup>
- Before taking on or continuing an outside business interest, making or holding a financial interest in a Scotiabank customer, supplier or service provider, or other entity having a close business relationship with Scotiabank, or committing to a job outside Scotiabank working hours, discuss this with your Manager to be sure these activities do not create a conflict. (Employees of securities or other subsidiaries may be subject to special rules with respect to outside employment, interests or activities and, therefore, may require pre-approval from their Compliance Department).

<sup>4</sup> Note: This is subject to any special policies or procedures that may be applicable to employees in certain job functions, business units or subsidiaries.

<sup>5</sup> This policy does not apply to holdings in the publicly traded securities of suppliers or customers, so long as Scotiabank policies with respect to misuse of confidential information and insider trading and tipping are complied with.

Introduction

Our guiding principles

Principle 1

## ▶ Principle 2

**Avoid putting yourself or Scotiabank in a conflict of interest position**

- I. Personal conflicts of interest
- II. Corporate conflicts of interest

Principle 3

Principle 4

Principle 5

Principle 6

Getting help or reporting problems and irregularities

Glossary

Key sources of guidance and advice

**d. Misuse of confidential information**

You are regularly entrusted with confidential information – information that is not or may not be publicly known – about Scotiabank, its customers and your fellow employees. This information is given to you so that you can do your job. It is wrong, and in some cases illegal, for you to access or use confidential information in order to obtain a personal benefit or to further your own interests. It is also wrong to disclose confidential information to any other person who does not require the information to carry out their job responsibilities on behalf of Scotiabank.

**e. Directorships**

**Obtaining Approval:** As an employee or officer, you may not accept a corporate directorship unless you have obtained approval from your Manager and the Compliance Department.<sup>6</sup> The Compliance Department will seek any other necessary approvals pursuant to the *Corporate Directorships Policy*. If you are a new employee, immediately report any directorships in accordance with these requirements, and seek approval where necessary. If you change your role within Scotiabank, advise your new Manager of any directorships, even if the directorship was previously approved. He or she can decide whether the prior approval must be reconfirmed, given your new duties.

Directorships of public companies are prohibited. Exceptions require the approval of the President & Chief Executive Officer of Scotiabank.

Also bear in mind that:

- Directorships on the boards of companies that compete with Scotiabank will not generally be approved; and
- Scotiabank reserves the right to require you to give up any directorships that it determines pose a conflict.

Scotiabank does not typically require that employees seek approval for the following kinds of directorships (on the presumption that they are unlikely to pose any conflicts):

- non-profit, public service corporations such as religious, educational, cultural, recreational, social welfare, philanthropic or charitable institutions or residential condominium corporations; and
- private, family-owned corporations (greater than 50%) incorporated to administer the personal or financial affairs of an officer or employee, or one or more living or deceased members of the officer's or employee's family (family includes spouses, parents, spouse's parents, children, grandchildren and spouses of children or grandchildren).

However, approval will be needed for certain employees that are registrants with certain regulatory authorities (e.g. IIROC). The Bank may attach specific conditions to any approval to address concerns including the management of potential conflicts of interest.

**Additional Reporting Requirements for VPs and Above:** While permission is not required, all employees at the VP level and above must, however, report directorships in non-profit or family-owned corporations to their Manager and the Compliance Department.<sup>7</sup>

For further guidance, refer to the *Corporate Directorships Policy*.

<sup>6</sup> Scotiabank may ask an officer or employee to act as a director of a subsidiary, affiliate or another corporate entity where it determines such a directorship to be in Scotiabank's interests. These directorships must be approved in accordance with applicable policies, procedures and processes.

<sup>7</sup> Note: You are not required to report a directorship of a family-owned corporation whose sole purpose is to own the home in which you reside.

[Introduction](#)[Our guiding principles](#)[Principle 1](#)

▶ **Principle 2**  
**Avoid putting yourself or Scotiabank in a conflict of interest position**

- I. Personal conflicts of interest
- II. Corporate conflicts of interest

[Principle 3](#)[Principle 4](#)[Principle 5](#)[Principle 6](#)[Getting help or reporting problems and irregularities](#)[Glossary](#)[Key sources of guidance and advice](#)

### f. Wills, other trusteeships and similar appointments

Customers sometimes try to express appreciation to employees through legacies, bequests or appointments in their wills. We expect you to decline any customer who suggests leaving you a gift in their will, as this could create a perception that you manipulated or took advantage of the customer.

You should never solicit from, or accept a personal appointment by, a customer as an executor, administrator or trustee, with some exceptions made for family relationships.

If you are named as a beneficiary, executor, administrator or trustee of a customer's will or some other trust document, other than as a family member, report the gift or appointment and the nature of the relationship to your Manager, who will consult the Compliance Department to determine an appropriate course of action. You will need management approval if you are to have signing authority for the estate's bank accounts. (Some affiliates and subsidiaries may require additional approvals.)

### g. Purchasing Scotiabank assets or administered or repossessed property

To avoid the appearance that Scotiabank is giving its employees an advantage, you or members of your household may not purchase Scotiabank assets such as automobiles, office equipment or computers, unless:

- the purchase is made at an advertised public auction;
- it has otherwise been established to Scotiabank's satisfaction that the price being paid is reasonable and your business unit head has approved the transaction; or
- the purchase is made under an approved Scotiabank program.

Similarly, neither you nor your family may use or purchase goods that have been repossessed by Scotiabank, except with the permission of your business unit head. He or she will review the situation and consider whether the transaction would both be, and appear to be, fair.<sup>8</sup>

### h. Related parties

Directors, certain senior officers, their spouses and minor children, as well as certain other entities such as companies which they control, are referred to as "related parties" (or "connected parties" in some countries) and there are laws governing their dealings with Scotiabank. If you have been advised that you are a "related party", you must abide by the policies and procedures which have been put in place to meet applicable legal requirements.

<sup>8</sup> If you work for a securities subsidiary, or any other subsidiary or area where a fiduciary obligation may be imposed by law, you may not use, or become the owner of, property held in fiduciary accounts under administration, unless you or a family member are a beneficiary or co-trustee of an estate and the governing document specifically permits you to use, or become the owner of, the property being administered.

- Introduction

---

- Our guiding principles

---

- Principle 1

---

- ▶ **Principle 2**  
**Avoid putting yourself or Scotiabank in a conflict of interest position**

  - I. Personal conflicts of interest
  - II. Corporate conflicts of interest

---

- Principle 3

---

- Principle 4

---

- Principle 5

---

- Principle 6

---

- Getting help or reporting problems and irregularities

---

- Glossary

---

- Key sources of guidance and advice

**II. Corporate conflicts of interest**

Conflicts of interest can also occur between Scotiabank and its customers. For example:

- Scotiabank’s interests could conflict with its obligations to a customer; or
- Scotiabank’s obligations to one customer could conflict with its obligations to another.

If you are a lending or advisory officer, be alert to situations where there may be a conflict or the appearance of one. If you become aware of a potential conflict, observe policies, procedures, and processes regarding confidentiality and advise your Manager or Compliance contact as set out in the *Key Sources of Guidance Advice Addendum* to ensure the situation is managed appropriately.

**a. Political contributions**

To avoid conflict of interests with political or state entities, Scotiabank in accordance with the Political Contributions Policy will not make corporate contributions to any political party. Scotiabank executives are also not permitted to use Bank resources or the Bank’s name to help organize, promote or host political fundraisers.

**Sample potential corporate conflicts of interest**

Situation	Conflict
Scotiabank is financing a customer who is unaware that they will be investing in another customer who is in financial difficulty, and investment proceeds will be used to pay down Scotiabank loans.	Risk of being perceived to have improved Scotiabank’s position at the expense of a customer.
Scotiabank is asked to lead financings for more than one customer’s bid for the same asset.	Risk of being perceived to have given one customer preferential treatment over another, or to have passed information to a customer’s competitor.

[Introduction](#)[Our guiding principles](#)[Principle 1](#)[Principle 2](#)**▶ Principle 3**  
**Conduct yourself honestly and with integrity**

- I. Illegal or fraudulent activities
- II. Improper transaction prevention
- III. Ethical business practices
- IV. Engaging third parties
- V. Communications and representations
- VI. Cooperate with audits and investigations

[Principle 4](#)[Principle 5](#)[Principle 6](#)[Getting help or reporting problems and irregularities](#)[Glossary](#)[Key sources of guidance and advice](#)

Our success depends on the honesty and integrity of Scotiabank employees, directors and officers. Always remember that your conduct has a direct effect on how customers think about Scotiabank.

**I. Illegal or fraudulent activities****a. Misappropriation**

Stealing customer or Scotiabank funds or information, attempting to defraud a customer or Scotiabank, or colluding with or knowingly helping others to do so are grounds for termination of your employment for cause and possible civil or criminal liability. This includes, but is not limited to, falsifying your expense claims, misuse of employee benefits such as employee banking privileges (including purchasing foreign currency for anyone other than eligible dependents) and corporate credit cards, or manipulating Scotiabank's clearing or payments systems (including but not limited to cheque writing, internet banking and ABMs) or General Ledger accounts to obtain credit or funds not rightfully yours.

You must follow Scotiabank's expense policies and procedures governing authorization and reimbursement of reasonable employment expenses, including the Scotiabank Travel Policy.

**b. Improperly accessing records, funds or facilities**

Never use your access to Scotiabank funds or facilities to do something improper. You may access, accumulate data and use records, computer files and programs (including personnel files, financial statements, online customer and employee profiles and other customer or employee information) only for their intended, Scotiabank-approved purposes.

You may not access or use Scotiabank facilities on behalf of third parties or for unreasonable or frequent personal use. Limited use of Scotiabank mailroom facilities to send or receive personal postal mail is permitted.

Nor may you access customer information for personal reasons or to provide the information to a third party unless this disclosure is authorized by Scotiabank. See Principle 4, Privacy and Confidentiality, for more guidance.

**c. Creating false records**

Forgery – even when not intended to defraud – is a crime, a betrayal of customer trust and a serious violation of this Code. You may not, under any circumstances, create a false signature or knowingly make or allow false or misleading entries to be made to any Scotiabank account, record, model, system or document.

Undisclosed or unrecorded Scotiabank accounts, funds, assets or liabilities are strictly prohibited. Immediately report your knowledge or discovery of any such account or instrument using one of the options in the *Pathways to Resolution guide* (or, where appropriate, under the *Whistleblower Policy*).

**Improperly accessing records**

You may not use your access to Scotiabank systems or facilities for non-business purposes.

For example, you may not view the account or personnel records of another employee or customer for personal reasons, or share contact details or financial information about a customer with third parties, such as mortgage brokers.

Any access to Bank records without authorization is a breach of this Code and may subject you to discipline, up to and including termination.

[Introduction](#)[Our guiding principles](#)[Principle 1](#)[Principle 2](#)**▶ Principle 3**  
**Conduct yourself honestly and with integrity**

- I. Illegal or fraudulent activities
- II. Improper transaction prevention
- III. Ethical business practices
- IV. Engaging third parties
- V. Communications and representations
- VI. Cooperate with audits and investigations

[Principle 4](#)[Principle 5](#)[Principle 6](#)[Getting help or reporting problems and irregularities](#)[Glossary](#)[Key sources of guidance and advice](#)**d. Bribes, payoffs and corrupt practices**

Scotiabank prohibits taking or offering bribes, kickbacks, extraordinary commissions, facilitation payments or any other improper kind of payment or benefit from or to suppliers or service providers, customers, public officials or others in exchange for favourable treatment or consideration.

Dealers, lawyers, consultants, brokers, other professionals, suppliers and service providers should be selected on the basis of qualifications, product or service quality, price and benefit to Scotiabank. Refer any offers or suggested payoffs to your Manager for investigation.

For additional guidance on Scotiabank's policies with respect to the prevention of bribery and corruption, refer to the *Anti-Corruption Policy*. You may also contact [business.conduct@scotiabank.com](mailto:business.conduct@scotiabank.com) for further advice or guidance.

**Trading restrictions and monitoring**

Regardless of your knowledge, in some circumstances Scotiabank may impose trading prohibition periods or other restrictions applicable to you. If your job makes it likely that you may encounter inside information, Scotiabank can also require that you do your securities trading only through brokerage accounts monitored by Scotiabank as well as impose other rules. These rules are to help protect you and Scotiabank.

**e. Insider trading and tipping**

In the course of your duties, you may become aware of confidential business information about Scotiabank or another public company. Some confidential information is sensitive enough that, if other people knew it, they would consider it important in deciding whether to buy or sell that company's securities, or it could be reasonable to expect that the price of the securities would be significantly affected. This kind of information is commonly called inside information.

You also may not pass on (or "tip") inside information about Scotiabank or any other public company to anyone except those persons who need to know that specific information in the necessary course of business. This activity is commonly called tipping.

There are very strict laws forbidding both insider trading and tipping, and violations carry severe penalties. Basically, these laws require that, if you have knowledge of inside information, you may not buy or sell (for yourself or for anyone else) stocks, bonds or other securities issued by that company (including derivatives linked to that company's securities), nor may you suggest or induce anyone else to do so.<sup>9</sup>

Employees likely to encounter inside information should become familiar with the specific policies and procedures that Scotiabank and its subsidiaries have put in place to restrict access to inside information, including information barriers. The Compliance Department is also available to provide you with advice.

**f. Other trading restrictions**

Employees, directors and officers of Scotiabank are prohibited under provisions of the *Bank Act* from trading in calls or puts (i.e. options to buy or sell shares at a set price) of Scotiabank shares.

Additionally, you may not short Scotiabank shares (i.e. you cannot sell securities you do not own). See the *Scotiabank Employee Personal Trading Policy* for further guidance.

<sup>9</sup> Where permitted by the Compliance Department, sales and trading staff may continue to accept unsolicited orders from clients.

[Introduction](#)[Our guiding principles](#)[Principle 1](#)[Principle 2](#)**▶ Principle 3**  
**Conduct yourself honestly and with integrity**

- I. Illegal or fraudulent activities
- II. Improper transaction prevention
- III. Ethical business practices
- IV. Engaging third parties
- V. Communications and representations
- VI. Cooperate with audits and investigations

[Principle 4](#)[Principle 5](#)[Principle 6](#)[Getting help or reporting problems and irregularities](#)[Glossary](#)[Key sources of guidance and advice](#)**g. Requirement to disclose a criminal charge or conviction**

You are required to disclose to Scotiabank if you are charged or convicted of theft, fraud or any other criminal offence in a domestic, foreign or military court. If you are charged with or convicted of an offence of this type, you must disclose it immediately to your Manager, who will consult Employee Relations or the local Human Resources department for further direction.

**h. Illegal or anti-competitive sales practices**

To promote fair and open competition among businesses in similar industries, many countries have competition laws or trade regulations, with severe penalties for violation.

Do not collude or co-operate with any other institution in anti-competitive activities. These include arrangements for or discussions intended to influence market prices, rates on key market interest rate or commodity indexes or on publicly traded equities, or about interest rates on loans and deposits, service fees, other product features or types or classes of persons to whom services will be made available or withheld.<sup>10</sup>

You may participate in industry associations, such as local Bankers Associations, to develop industry positions on legislative or other issues, or to set standards for the use of common facilities or networks. However, these meetings must not be used to discuss competitive policies and practices. If you have any doubt whether a discussion would violate competition laws, do not participate and consult with your Manager or the Legal Department.

<sup>10</sup> Note: Some permitted exceptions are discussions regarding syndicated loans, underwritings and other kinds of authorized consortia, and certain government lending programs. In these cases, limit discussions to the specific transaction or program.

**II. Improper transaction prevention****a. Know your customer/understand your customer's transaction**

Knowing our customers and understanding our customers' transactions are fundamental tenets of the financial services industry. Knowing our customers helps us to better serve customer needs, identify sales opportunities, meet regulatory requirements, avoid facilitating unethical behaviour and protect ourselves during disputes and litigation. It also allows us to contribute to national and global efforts to combat criminal and terrorist activity.

All transactions must be authorized and handled in an approved manner, and must adhere to applicable standards for knowing your customer. Do not undertake, participate in or facilitate any customer transactions that are prohibited by law, regulation or policy or that, by Scotiabank's standards, could be considered improper or suspect.

**b. Detecting and reporting suspicious or improper transactions**

You should familiarize yourself with the policies, procedures and processes related to anti-money laundering and anti-terrorist financing. Be alert to any illegal, suspicious or unusual activity, including fraud, money laundering, terrorist financing or breach of government-imposed sanctions requirements.

Promptly report any unusual account activity to your Manager or, in the case of suspected money laundering or terrorist financing, your designated Anti-Money Laundering Compliance Officer. If you fail to report a transaction that there are reasonable grounds to suspect is associated with money laundering or terrorist financing, you may be committing a criminal offence. It is also a breach of this Code, and an offense in many jurisdictions, to warn a customer that a report has been made about them or their activities.

Introduction

Our guiding principles

Principle 1

Principle 2

▶ **Principle 3**  
**Conduct yourself honestly and with integrity**

- I. Illegal or fraudulent activities
- II. Improper transaction prevention
- III. Ethical business practices
- IV. Engaging third parties
- V. Communications and representations
- VI. Cooperate with audits and investigations

Principle 4

Principle 5

Principle 6

Getting help or reporting problems and irregularities

Glossary

Key sources of guidance and advice

### III. Ethical business practices

#### a. Offering and accepting gifts and entertainment or charitable donations or sponsorships

Customers and business associates often try to show their appreciation by providing gifts and entertainment to Scotiabank employees or by making charitable donations to a charity on behalf of, or through sponsorship of, an employee. Similarly, Scotiabank employees may wish to show their appreciation to our clients and suppliers by offering gifts and entertainment or making charitable donations to a charity on behalf of, or through sponsorship of, a customer or business associate. Offering or accepting gifts or entertainment or charitable donations or sponsorships can be problematic because it may lead others to believe that your decisions have been improperly influenced. In some cases, such as where high-value gifts or entertainment have been offered or accepted, this could be perceived as offering or accepting a bribe.

In general, the giving and accepting of gifts and entertainment or making charitable donations or sponsorship is only permitted if:

- the gift, donation or sponsorship is modest and would not affect the recipient's objectivity;
- there is no suggestion that the donor is trying to obligate or improperly influence the recipient;
- offering or accepting is "normal business practice" for the purposes of courtesy and good business relations;
- offering or accepting is legal and consistent with generally understood ethical standards;

- neither you nor Scotiabank would be embarrassed if the public became aware of the circumstances of the gift or entertainment, donation or sponsorship;
- it is not a gift or prize of cash, bonds, negotiable securities, personal loans, or other valuable items (such as airline tickets for your personal use, or use of a vacation property).

Before offering or accepting entertainment involving air travel, luxury accommodation or exclusive tickets (such as to the Olympics, US Open, Wimbledon or the World Cup), obtain the approval of your business unit group head (or his or her designate), who must consult their Compliance Department for further guidance.

Remember the following when considering whether to **accept a gift** or entertainment or donation to a charity on your behalf or through sponsoring you:

- You may not use your position for improper personal gain. Tactfully discourage customers, brokers, suppliers or others in business with Scotiabank if they suggest offering benefits to you or your family.
- You should not accept any donations on your behalf, or sponsorships, for charities for which you are in some way associated other than donations or sponsorships of nominal amounts.
- Where it would be extraordinarily impolite or otherwise inappropriate to refuse a gift of obvious value, you may accept it on behalf of Scotiabank. In these cases, immediately report the gift to your Manager who will advise you how to deal with it. Such gifts may not be taken for your personal use or enjoyment.

Remember the following when considering whether to **offer a gift** or entertainment or donation or sponsorship to a charity:

- Be especially careful when offering gifts or entertainment to public officials or making charitable donations on a public official's behalf or at his or her request. Many countries have strict laws regarding offering anything of value to these individuals or to third parties at their request. Please also refer to any specific policies within your business unit relating to the offering of gifts or entertainment.
- Always comply with the Anti-Corruption Policy in any dealings with public officials. Gifts to, or entertainment of, public officials that exceed US\$100 in value will require additional approvals as set out in the Anti-Corruption Policy.

[Introduction](#)[Our guiding principles](#)[Principle 1](#)[Principle 2](#)**▶ Principle 3****Conduct yourself honestly and with integrity**

I. Illegal or fraudulent activities

II. Improper transaction prevention

## • III. Ethical business practices

IV. Engaging third parties

V. Communications and representations

VI. Cooperate with audits and investigations

[Principle 4](#)[Principle 5](#)[Principle 6](#)[Getting help or reporting problems and irregularities](#)[Glossary](#)[Key sources of guidance and advice](#)

Subject to the special considerations discussed below relating to government officials and public office holders (“public officials”), examples of the types of gifts and entertainment, or charitable donations or sponsorships that are acceptable to offer or accept include:

- occasional meals, refreshments, invitations to local events;
- small, occasional gifts for special occasions such as an anniversary, significant event or holiday;
- inexpensive advertising or promotional materials, such as pens or key chains;
- inexpensive awards to recognize service and accomplishment in civic, charitable, educational, or religious organizations;
- donations on behalf of, or sponsorships of, individuals of modest or nominal amounts;
- modest honoraria and reimbursement for reasonable expenses (if not paid by Scotiabank) for Scotiabank-related speaking engagements or written presentations; or
- gifts or entertainment or charitable donations or sponsorships clearly motivated by obvious family or close personal relationships, rather than business dealings.

Depending on the monetary value of the item, you may wish to consult with your Manager regarding the appropriateness of the gesture. Your Manager can consult with the Compliance Department for guidance on difficult situations.

**Coercive tied selling**

Never pressure a customer to buy a product or service that he or she does not want as a condition for obtaining another product or service from Scotiabank. (This practice, which is illegal in some jurisdictions, is sometimes called coercive tied selling).

This should not be confused with other practices, such as giving preferential pricing to customers who already have business with Scotiabank or bundling products and services. These practices are legal and accepted in some countries, but may be illegal in others, so ensure that you are aware of all applicable local laws.

**b. Dealing ethically with our customers, employees and others**

As Scotiabankers, we do not compromise our ethics for the sake of meeting our sales, profit or other targets or goals. Steering a customer to an inappropriate or unnecessary product harms the customer, damages our reputation and may be illegal in certain situations and jurisdictions.

Never take unfair advantage of anyone through manipulation, concealment, abuse of confidential business or personal information, misrepresentation of material facts, or any other unfair-dealing or unethical business practice.

If you discover misrepresentations or misstatements in information provided to customers or the public, consult your Manager about how to correct those statements.

All applicants for employment at any level within Scotiabank must be considered based on qualification and compensation must be appropriate for the work being performed and should be consistent with the compensation paid to other employees for similar work. Never give preferential treatment in hiring, promotion, or compensation decisions to individuals based on their

family, political, governmental or other affiliations.

The employment of a Politically Exposed Person, or a family member or known contact of a public official, could give rise to a perception that favourable treatment has been bestowed upon such an individual and could put you and Scotiabank at risk of breaking the law. It is important to be aware of Scotiabank’s relationship with public officials (for example, where Scotiabank is in the process of applying for a license from an official’s department) and how the employment by Scotiabank of a family member or contact of an official could be perceived.

Never seek to obtain personal advantages from your customer or other business relationships. For example, do not:

- use your connection with Scotiabank so that you or your family can borrow from or become indebted to customers; or
- use your position to gain preferred rates or access to goods and services<sup>11</sup>, whether for you personally or for friends or relatives, unless the benefit is conferred as part of a Scotiabank-approved plan available to all or designated groups of employees.

<sup>11</sup> For example: Do not use your position to gain access to trading facilities or opportunities to further your personal investments, such as gaining access to new stock issues or hard-to-get securities.

[Introduction](#)[Our guiding principles](#)[Principle 1](#)[Principle 2](#)**▶ Principle 3**  
**Conduct yourself honestly and with integrity**

- I. Illegal or fraudulent activities
- II. Improper transaction prevention
- III. Ethical business practices
- IV. Engaging third parties
- V. Communications and representations
- VI. Cooperate with audits and investigations

[Principle 4](#)[Principle 5](#)[Principle 6](#)[Getting help or reporting problems and irregularities](#)[Glossary](#)[Key sources of guidance and advice](#)**c. Respect intellectual property rights**

We respect and avoid the unauthorized use of others' intellectual property rights.

You may not download any third-party intellectual property – including software, creative works or other materials – if to do so would violate any vendor/owner rights. Be aware that software available over the Internet, including free and demo software, and upgrades to software already in use, may have licensing restrictions which are not readily apparent.

When using supplier or service provider and third party systems and programs, comply with the licensing, confidentiality and registration requirements. For example, do not share your registration information for external databases with others as this would be a breach of the licensing and copyright terms of your subscription or would violate any vendor/owner rights. Failure to respect these requirements could subject you or Scotiabank to serious penalties.

When using the Internet, always comply with this *Code*, which contains guidance on respecting intellectual property laws.

If you develop, as part of your work for Scotiabank or with the use of Scotiabank facilities, any patentable invention, industrial design or creative work, it belongs to Scotiabank unless a specific exception has been made.

**IV. Engaging third parties**

In conducting business, Scotiabank uses suppliers or service providers and contractors and may enter into outsourcing arrangements or other strategic alliances. If you are authorized to engage third parties, you should engage only those who are competent and reputable, and who have business conduct standards comparable to our own, as these are critical considerations for Scotiabank. Engaging family members to act in such a capacity is considered a conflict of interest.

**V. Communications and representations**

Trust is the basis of our relationships with our customers, fellow employees, shareholders and the communities in which we operate. You must not knowingly mislead customers, the general public or other employees by making false or misleading statements or by withholding information.

**a. Advertising**

You should be aware that Scotiabank is subject to regulation with respect to advertising. If approving advertising is not part of your job, ensure that you follow established approval procedures or get the approval of your supervising office or department head before initiating any advertisements.

**b. Proper public disclosure**

Scotiabank is committed to providing timely, accurate, balanced and widely distributed disclosure of material information, as required by law or regulation. For additional information, consult the *Statement of Disclosure Policy and Practices and Mandate of the Disclosure Committee*. Refer inquiries from the financial community, shareholders and media to an authorized spokesperson.

[Introduction](#)[Our guiding principles](#)[Principle 1](#)[Principle 2](#)**▶ Principle 3**  
**Conduct yourself honestly and with integrity**

- I. Illegal or fraudulent activities
- II. Improper transaction prevention
- III. Ethical business practices
- IV. Engaging third parties
- V. Communications and representations
- VI. Cooperate with audits and investigations

[Principle 4](#)[Principle 5](#)[Principle 6](#)[Getting help or reporting problems and irregularities](#)[Glossary](#)[Key sources of guidance and advice](#)**c. Making public statements and media contact**

Unless you are authorized to speak to reporters or the media on behalf of Scotiabank as part of your normal duties, refer all media enquiries to a designated spokesperson. Be especially careful never to respond to questions about a matter where litigation is pending or in process (without prior authorization of the Legal Department) and always respect Scotiabank's duty of confidentiality to its customers, employees and others.

Sometimes employees are asked to give presentations or express views on matters generally relating to banking or other financial services, usually due to their position with Scotiabank or acknowledged expertise. Speaking opportunities at conferences and industry events should be treated as public events and you should expect that media may be in attendance or people may share the information you present in social media. Please ensure that your manager provides approval for any public speaking events you may participate in. Even if you are presenting in your own personal capacity and you've made that clear, please remember that by the nature of your title, the public may still interpret your views as Bank views. Think carefully about what you say and how you say it in any public forum.

**d. Expressing your personal views**

As a private citizen, you are entitled to express your personal views. However, be careful not to give the impression that you are speaking on behalf of Scotiabank or expressing Scotiabank's perspective, unless you have obtained approval from your Manager and/or an authorized spokesperson. This applies to all forms of communication (such as statements, speeches, letters or articles) and all communications media or networks (such as newspaper, radio, television, E-mail, social media or the Internet).

You should also bear in mind that your conduct outside the workplace may reflect on Scotiabank. Use common sense when offering your personal opinions in a public forum (such as social media, internet blogs, or newsgroups) and refrain from disparaging competitors or making statements that might discredit Scotiabank or its products and services. Also, take particular care not to disclose confidential information about Scotiabank, customers, employees or others.

**e. Use of the Scotiabank brand, name and reputation**

Our brand and reputation are significant corporate assets. They should only be used to further Scotiabank business. Never use Scotiabank's name, logo, letterhead or reputation to gain personal advantages or to further your own interests, or for anything other than approved purposes.

**VI. Cooperate with audits and investigations**

Always cooperate fully with any investigations by management or the Compliance, Legal, Internal Audit, Security and Investigation or Human Resource Departments. Be straightforward, candid and truthful when dealing with internal and external investigations, external auditors and regulators. However, keep in mind Scotiabank's confidentiality guidelines and procedures for releasing information.

You must not destroy, discard, withhold or alter records pertinent to a regulatory authority, an audit, a legal or governmental investigation.

## PRINCIPLE 4 | **Respect confidentiality, and protect the integrity and security of assets, communications, information and transactions**

Introduction

Our guiding principles

Principle 1

Principle 2

Principle 3

▶ **Principle 4**

**Respect confidentiality, and protect the integrity and security of assets, communications, information and transactions**

- I. Privacy and confidentiality
- II. Accuracy and integrity of transactions and records
- III. Security
- IV. Digital communications, use and representation

Principle 5

Principle 6

Getting help or reporting problems and irregularities

Glossary

Key sources of guidance and advice

### I. Privacy and confidentiality

You have an obligation to safeguard the personal and business information entrusted to us by customers, employees, suppliers, service providers and others, as well as the confidentiality of Scotiabank's own affairs. This obligation continues even after you leave Scotiabank.

#### a. Obligation to protect personal and confidential information

Customers, employees, suppliers, service providers and others trust Scotiabank to keep their personal information and confidential business information safe and secure. Protecting their privacy and the confidentiality of their dealings with us is essential to safeguarding our reputation. Protecting personal and confidential information is also a legal requirement.

You are expected to be aware of, and follow, the policies and procedures that Scotiabank has put in place to protect personal and confidential information and to comply with applicable laws and regulations, including the *Personal Information Privacy Protection Policy and Guidelines*. Those policies and procedures explain how to report, respond to and remediate a breach of privacy or confidentiality.

All information about, or received from, individual or business customers or employees (including prospective customers and employees) should be presumed to be confidential information unless the contrary is clear. Keep in mind that even a seemingly harmless or helpful disclosure of customer or employee personal information (such as to a customer's family member) could be a breach of this Code and can have serious consequences for you, Scotiabank and the customers involved.

Never access customer or employee personal information, or confidential business information about

Scotiabank or a customer, without a legitimate business reason and proper authorization. Employee "snooping" into files of customers or other employees is prohibited. For example, you may not view customer profiles or account information of family members, friends or acquaintances without a valid business reason to do so. Scotiabank monitors employees' access to and use of

information technology services and physical storage facilities in order to prevent and detect improper access to information. Employee snooping is a breach of the law and this Code, and could result in termination of employment and legal proceedings against you by Scotiabank and the affected individuals.



#### **Appropriate handling of personal and confidential information includes the following:**

- Follow policies, procedures and processes for storing and controlling access to electronic and physical confidential information.
- Follow any policies, procedures or processes for transmitting confidential information. Do not send confidential information via non-secure media such as fax, email, SMS/text, instant messaging or the Internet. Follow the secure email function procedures where confidential information must be sent outside Scotiabank. See *the Key Sources of Guidance and Advice* addendum for more information.
- Do not carelessly display confidential information (by, for example, leaving it visible on a computer monitor, or leaving confidential documents where they could be viewed, lost or stolen).
- Do not disclose confidential information to persons outside Scotiabank (including family or household members or close associates) or to other employees who do not require the information for their work.
- Take care when discussing confidential information where it might be overheard or intercepted (such as when using a cell phone) by, for example, being certain to whom you are speaking and ensuring that your conversation cannot be overheard by unauthorized persons. Never discuss confidential information in social settings, such as restaurants, elevators, trains and other public places.
- Destroy or dispose of information according to security requirements and policies and procedures for document retention and destruction.

PRINCIPLE 4 | **Respect confidentiality, and protect the integrity and security of assets, communications, information and transactions** *continued*

Introduction

Our guiding principles

Principle 1

Principle 2

Principle 3

► **Principle 4**

**Respect confidentiality, and protect the integrity and security of assets, communications, information and transactions**

- I. Privacy and confidentiality
- II. Accuracy and integrity of transactions and records
- III. Security
- IV. Digital communications, use and representation

Principle 5

Principle 6

Getting help or reporting problems and irregularities

Glossary

Key sources of guidance and advice

**b. Appropriate handling of personal and confidential information**

It is your responsibility to safeguard and appropriately handle any personal or confidential information which you have custody of or access to, or which you use. This is the case even when you are disposing of waste or damaged materials.

In order to appropriately safeguard personal and confidential information, you must ensure that any new Scotiabank initiative or service and any new use of personal information that you are involved with has undergone a Privacy Impact Assessment, a Security Threat/Risk Assessment and all suggested privacy and security protections are implemented, before it is launched.

If you become aware of a breach of privacy or confidentiality, immediately report it through one of the options described in the *Key Sources of Guidance and Advice* addendum to this Code, in the *Pathways to Resolution* guide or, where appropriate, under the *Whistleblower Policy*, so that steps can be taken to prevent, minimize or mitigate any negative impact on customers, employees or Scotiabank.

**c. Disclosures of personal and confidential information**

Third parties sometimes request information about customers (including family and friends). Subject to legal exceptions, you must obtain the consent of the customer before releasing a customer's personal or confidential business information. This includes releasing information about whether or not an individual, business or government department is actually a customer.

In some cases, you may need assistance from the Legal Department to verify if a demand for information has been properly made and documented to permit or compel you or Scotiabank to provide information under the law without customer consent. You should also be alert to situations where legal requirements may prohibit you from telling the customer about a demand for information.

**II. Accuracy and integrity of transactions and records**

The expectations of our customers, shareholders, regulators and other stakeholders make it essential that Scotiabank's books and records are complete and accurate.

All employees must play their part in ensuring the accuracy and integrity of our record-keeping and information reporting systems. Follow applicable policies, procedures, and processes to ensure that transactions:

- have a legitimate business purpose (e.g. the objective is not to achieve misleading earnings, revenue or balance sheet effect, mislead a regulator, or another unethical or illegal outcome);
- are properly authorized;
- are promptly and accurately recorded in the right accounts; and
- are adequately supported by back-up documentation.

Internal controls and procedures are in place to protect Scotiabank. Under no circumstances should you try to bypass an internal control, even if you think it is harmless or will save time. If you become aware that an internal control or procedure has been improperly bypassed or overridden, immediately report the incident using one of the options in the *Pathways to Resolution* guide (or, where appropriate, under the *Whistleblower Policy*.)

Introduction

Our guiding principles

Principle 1

Principle 2

Principle 3

## ▶ Principle 4

**Respect confidentiality, and protect the integrity and security of assets, communications, information and transactions**

I. Privacy and confidentiality

II. Accuracy and integrity of transactions and records

## • III. Security

IV. Digital communications, use and representation

Principle 5

Principle 6

Getting help or reporting problems and irregularities

Glossary

Key sources of guidance and advice

**III. Security****a. Keep Scotiabank and customer assets safe**

Be alert to the potential for harm, loss, corruption, misuse, unauthorized access or theft of Scotiabank or customer assets. These include:

- funds and negotiable instruments;
- physical property, premises, supplies and equipment;
- technological devices and resources such as computer systems and networks, telecommunication systems and access channels to E-mail and the Internet;
- intellectual property, including software developed by employees or provided by third parties; and
- personal and confidential information, however stored or maintained, including information held on electronic storage devices.

Be careful not to compromise security through the inappropriate disclosure of information or images, such as photographs. Never discuss or disclose the design or operation of systems or security protection processes or procedures with anyone outside or inside Scotiabank, other than on a need-to-know basis. Never use a public cloud service from a Scotiabank computer or device or to conduct any Bank business, unless the service has been approved by the designated committee (Cloud Governance Council).

Report any perceived weakness or deficiency in a system or security protection procedure to your Manager or other appropriate senior officers (e.g. Chief Information Security Officer).

**b. Integrity of computer and communication systems**

Computer systems, programs and other technological assets and resources must be protected from theft, unauthorized access or misuse, and intentional and unintentional loss or corruption. You must comply at all times with security policies, processes and protection requirements, including any specific requirements applicable to a system or program which you use. For example:

- use only Scotiabank-approved computer programs and software; and
- safeguard all access identifiers (e.g., passwords, access codes, badges), combinations, and physical keys in your custody; do not give, lend, share or duplicate them without authorization.

**c. Assets or information in the hands of third parties**

If you have authorized assets or personal or confidential information to be held in the custody or safekeeping of third parties, you are responsible for ensuring that their security procedures meet or exceed Scotiabank standards. This will typically involve ensuring contractual safeguards are in place with assistance of the Legal Department and that a Threat & Risk Assessment has been conducted with the assistance of Information Security & Control.

**d. Use of Scotiabank property and information off-premises**

When you work at home or off-site, whether occasionally or as part of an approved arrangement, and have Scotiabank assets in your custody, you are expected to keep those assets safe by knowing and following security policies and procedures. When working at home or off-site:

- consider the sensitivity of information before taking it off-premises, whether in hard copy or electronic format, and take only the minimum information required;
- ensure all confidential information is safeguarded from unauthorized access, theft, misuse, loss or corruption in keeping with applicable policies, procedures and processes; and
- never copy Scotiabank information for your or someone else's non-work-related use without authorization.

Except as may be required for working at home or offsite, files or other information are not to be removed from Scotiabank premises without authorization.

**e. Appropriate use of information technology and services**

Electronic and telecommunications facilities and systems, such as computers, Internet access, voice mail, E-mail, fax machine and telephone, are provided to you to enable you to do your job. Any other use, except for reasonable and occasional use, is not allowed. Scotiabank information technology services are monitored for inappropriate use.

Introduction

Our guiding principles

Principle 1

Principle 2

Principle 3

## ▶ Principle 4

**Respect confidentiality, and protect the integrity and security of assets, communications, information and transactions**

I. Privacy and confidentiality

II. Accuracy and integrity of transactions and records

III. Security

- IV. Digital communications, use and representation

Principle 5

Principle 6

Getting help or reporting problems and irregularities

Glossary

Key sources of guidance and advice

#### IV. Digital communications, use and representation

Inappropriate internet use outside the workplace could subject Scotiabank or its employees or customers to legal, reputational, privacy, security or other risks. If you choose to offer your personal opinions online, use common sense and be careful not to give the impression you are speaking on behalf of Scotiabank or expressing a Scotiabank-approved perspective.

Scotiabank's policy is to be truthful and non-misleading in all communications and representations, written and verbal. This includes communications by e-mail, or using web-based public forums such as internet "blogs", chat rooms, newsgroups, social media etc. (otherwise known as 'digital communications').

Some rules to follow when using digital communications include the following:

- Always use appropriate and professional language;
- Consider the appropriateness of using Scotiabank e-mail as a point of contact for third parties;
- Unless you are a specially designated person for whom it forms part of your normal duties, refrain from commenting on Scotiabank, its business activities or competitors in any online public forum;
- Never post material obtained from or associated with Scotiabank that is damaging to the interests of or embarrassing to Scotiabank;
- Do not use Scotiabank logos, trademarks, trade name or other proprietary materials without prior approval or for any purpose other than the furtherance of Scotiabank's legitimate business objectives. Ensure that you follow Scotiabank, subsidiary or business line guidelines when using Scotiabank logos, trademarks, trade names online;
- Do not promote specific Scotiabank products and services as these may require certain mandatory disclosures when targeted at the public;
- Under no circumstances may inside or confidential information – including information about customers, employees or Scotiabank – be posted to any public or non-Scotiabank sites. This includes information on Scotiabank's security procedures, practices or vulnerabilities, as well as images or representations of Scotiabank facilities;
- Ensure that you do not compromise the confidential information of customers, employees or Scotiabank; and
- Be alert for fraudulent activities and social engineering techniques. Social Engineering is a collection of techniques used to trick employees into divulging confidential personal or business information or granting access to secure systems.

When you use Scotiabank assets to communicate over its electronic networks, to discuss Bank related matters or to access the internet for personal or business related use, you must also comply with the following provisions:

- All e-mails sent to a third party from a Scotiabank network must be sent in a bank approved, secure manner and in compliance with applicable policies, procedures and processes;
- Employees must not use personal e-mail accounts for business purposes – do not send or forward Bank confidential information to these accounts; and
- When Scotiabank communicates through digital communications such as social media or e-mail it is important to ensure that only specifically approved employees may participate and have access to digital communication use.

Personal use of external or internal digital communications should be done responsibly. You should never provide financial advice online, use Scotiabank logos or trademarks as part of your personal postings or promote rates, fees or services. You should also never disclose confidential information, results, strategy or other internal information of Scotiabank and ensure that competitors, customers or colleagues are never discussed.

As an employee of the Bank, you represent the Bank in all digital communications sent internally or externally for business or personal use at and outside of work. When using social media, e-mail or other digital communication methods consider the potential impact on Scotiabank's brand, image and reputation. Scotiabank's expectations apply to all employees wherever we happen to be; whether in a Scotiabank workplace or not.

Introduction

Our guiding principles

Principle 1

Principle 2

Principle 3

Principle 4

▶ Principle 5

**Treat everyone fairly, equitably, and professionally**

- I. Diversity, equity and human rights
- II. Workplace health and safety

Principle 6

Getting help or reporting problems and irregularities

Glossary

Key sources of guidance and advice

### **Treat everyone fairly, equitably, and professionally whether they are customers, employees, shareholders, suppliers, service providers, governments, regulators, competitors, the media or the public**

Scotiabank is committed to respecting human rights and treating all current and potential employees, customers, shareholders, suppliers, service providers, governments, regulators, competitors, the media and the public fairly, and to maintaining a work environment that supports the productivity, personal goals, dignity and self-respect of all employees.

This includes commitments to:

- the creation and support of a work force, at all levels of the organization, that reflects the diverse population of the communities it serves; and
- providing reasonable accommodation to permit qualified persons who face some barrier (e.g. persons with disabilities) to do their jobs.

### **I. Diversity, equity and human rights**

#### **a. Harassment and discrimination**

Every employee is entitled to harassment-free employment. Every customer is entitled to harassment-free financial services. Scotiabank is committed to complying with the spirit and intent of *The Canadian Human Rights Act* and other human rights and anti-discrimination laws that apply to subsidiaries or to Scotiabank's operations outside of Canada. The actions of all directors, officers and employees are expected to be consistent with these principles.

Harassment, including sexual harassment, is a form of discrimination. Harassment means any conduct, comment, gesture, or contact related to prohibited grounds of discrimination:

- that is likely to cause offence or humiliation to any employee or customer (for example, bringing images or text of a sexual nature into the workplace, or making discriminatory or sexualized jokes or remarks); or
- that might reasonably be perceived as placing a condition of a discriminatory nature on employment or employment opportunities such as training or promotion, or on the provision of financial services.

Complaints of harassment or discrimination will be dealt with promptly, and treated with seriousness, sensitivity and confidentiality. Never retaliate against any employee for having raised concerns or complaints in good faith.

For more information on Scotiabank's policies with respect to harassment and discrimination, refer to the *Human Rights Policy*.

### **II. Workplace health and safety**

Scotiabank is committed to providing its employees with a healthy, safe workplace, in compliance with applicable local laws and regulations. This includes a commitment to providing a workplace that is free from violence by maintaining a respectful, non-threatening work environment.

You have an important role to play in creating and maintaining our healthy and safe work environment by:

- becoming familiar with your roles and responsibilities with respect to health and safety, and acquiring the necessary training to fulfill those roles and responsibilities;
- reporting any condition or practice that you believe may be hazardous using one of the options in the Pathways to Resolution guide (or, where appropriate, under the Whistleblower Policy); and
- treating all those you deal with respectfully and professionally, and never acting in a violent, threatening or abusive manner.

Employees who hold managerial or supervisory roles may have additional health- and safety-related responsibilities and should be guided by any supplementary requirements of their local business unit, as applicable.



Introduction

Our guiding principles

Principle 1

Principle 2

Principle 3

Principle 4

Principle 5

## ▶ Principle 6

Honour our commitments to the communities in which we operate

- I. Environmental protection
- II. Charitable and community activities
- III. Political activities
- IV. Other codes of conduct and voluntary commitments

Getting help or reporting problems and irregularities

Glossary

Key sources of guidance and advice

To succeed, we must all act in a manner that is environmentally, economically and socially responsible. Doing so will ensure that we are viewed as a welcome partner in the markets in which we operate, and those we seek to enter.

### I. Environmental protection

As a major international financial institution, our day-to-day operations have a number of direct and indirect impacts on the environment. Scotiabank has taken steps to mitigate these impacts by adopting policies, procedures and processes with respect to, for example, environmental credit risk, responsible environmental management of our real estate holdings and enhanced social and environmental guidelines for project finance loans in developing countries.

Employees are expected to be aware of and comply with those policies, procedures and processes that apply to their area of responsibility.

### II. Charitable and community activities

We are committed to making a positive contribution to the communities in which we operate. All donations or support given on behalf of Scotiabank should be made in accordance with applicable policies, procedures and processes.

In special cases, your Manager or another senior officer may approve the use of Scotiabank equipment, facilities or staff time for charitable activities. Otherwise, as much as possible, you should limit charitable and community activities to non-business hours.

#### Charitable Donations

When soliciting charitable donations or support, whether on behalf of Scotiabank or another organization, you should emphasize the voluntary nature of the donation or support. No one should feel pressured to contribute to fundraising campaigns and/or under no circumstances are you permitted to give preferential treatment to employees who may contribute to solicited charities.

### III. Political activities

#### a. Political activities and donations in the name of Scotiabank

Scotiabank will not make political donations, to avoid conflict of interests with political or state entities.

Scotiabank does not make political donations as these might be interpreted as an attempt to encourage favourable treatment of the Bank or a subsidiary.

#### b. Personal political participation

Scotiabank considers its employees' participation in the political process to be an important contribution to the community and a personal decision that is subject to their conscience and individual discretion. No one in Scotiabank may require an employee, director or officer to:

- personally contribute to, support or oppose any candidate or political organization; or
- refrain from personal political activity, providing that activity is not prohibited by law and is not conducted on Scotiabank's time or using its facilities or resources, does not interfere with job performance, and does not present a conflict of interest for the employee, director or officer.

However, the time and attention devoted to these activities should not interfere with your job performance, or present any other kind of conflict. Before you run for office or accept a political appointment, discuss your intention with your Manager to ensure there will not be a conflict.



When engaging in personal political activities outside of work, make it clear that those activities are not being conducted on behalf of Scotiabank. The use of Scotiabank equipment, facilities, staff or other resources to conduct political activities is prohibited, unless explicitly authorized by the President & Chief Executive Officer of Scotiabank or your subsidiary.

### IV. Other codes of conduct and voluntary commitments

#### a. Commitments by Scotiabank

It is important that we honour our public commitments and adhere to other codes of conduct and voluntary undertakings to which Scotiabank has agreed to be bound. Employees are expected to be aware of and comply with those codes and public commitments that apply to their area of responsibility.

#### b. Professional codes of conduct

Many professions and professional bodies have codes of conduct or ethics to which they expect their members to adhere. If you come across an instance where your profession's code of conduct conflicts with this Code, inform your Manager and the Compliance Department immediately. In most cases, you should follow the more stringent requirement to the extent the conflict exists.

# Getting help or reporting problems and irregularities

Introduction

Our guiding principles

Principle 1

Principle 2

Principle 3

Principle 4

Principle 5

Principle 6

► **Getting help or reporting problems and irregularities**

- I. Obligation to report
- II. Protection from retaliation
- III. How to report

Glossary

Key sources of guidance and advice

## I. Obligation to report

Immediately report any actual, suspected or potential violations of law, regulations, or internal policies (including instances where you see a risk that appears to have been overlooked or ignored by others).

Reporting such matters can help protect you and Scotiabank, as well as other employees, customers, shareholders and other stakeholders. If you believe that you may have breached this Code, a policy, procedure, code of conduct that applies to you or potentially violated any law or regulation you have an obligation to report it to your Manager immediately. Failing to do so is grounds for immediate termination for cause.

You also have an obligation to Scotiabank, other employees, directors, officers and yourself to report:

- a breach or suspected breach of this Code or supplemental guidelines by another employee, director or officer;
- a weakness or deficiency in Scotiabank's policies, procedures, processes or controls that might enable breaches to occur or go undetected; and
- any failure of a supplier, service provider or contractor to adhere to legal requirements or ethical standards comparable to this Code.

If a problem or irregularity has been referred to you, resolve the issue or refer it appropriately using one of the options in the *Pathways to Resolution* guide (or, where appropriate, under the *Whistleblower Policy*).

## II. Protection from retaliation

Scotiabank will protect from retaliation any employee, director or officer who, in good faith, reports actual or suspected breaches of this Code or violations of law, regulations or internal policies by another director, officer or employee, supplier, service provider or contractor, or problems with Scotiabank's policies, procedures, processes or controls.

Retaliatory action of any kind against an employee, director or officer who makes a report in good faith could be grounds for termination for cause and may be subject to criminal or civil penalties.

Scotiabank further protects employees by providing a number of anonymous and confidential methods for the disclosure of wrongdoing or irregularity (see next page).

# Getting help or reporting problems and irregularities

Introduction

Our guiding principles

Principle 1

Principle 2

Principle 3

Principle 4

Principle 5

Principle 6

► **Getting help or reporting problems and irregularities**

I. Obligation to report

II. Protection from retaliation

• **III. How to report**

Glossary

Key sources of guidance and advice

## III. How to Report

### a. Pathways to Resolution guide

You should report any breach or suspected breach of this Code to your Manager or any Manager as set out in the *Pathways to Resolution* guide (or, where appropriate, under the *Whistleblower Policy*). Consult a more senior officer if you do not receive what you consider to be a reasonable response from the first person. Employees can also report harassment or other workplace issues to the Employee Relations Department through their local Human Resources Call Centre, or to their local Human Resources department or representative.

Breaches or suspected breaches of this Code will be dealt with promptly and fairly. However, if you do not feel your complaint or concern has been appropriately resolved, there are other, alternative options available to you (see below).

### b. Alternative, confidential avenues

It may not always be appropriate or adequate to report breaches or concerns through the “Open Door” options described in the *Pathways to Resolution* guide. (For example, you may be concerned about the possibility of reprisal by persons involved in a breach or suspected breach of this Code). Scotiabank has therefore created alternative, confidential avenues to disclose breaches, problems and irregularities:

- The *Whistleblower Policy* outlines the process for reporting accounting and auditing concerns, suspected fraudulent activity, breaches of this Code or other Compliance policies, and whistleblowing retaliation and retribution. It includes information on how to report anonymously. Concerns may be raised in writing directly with Scotiabank’s Chief Auditor, or via Global Compliance Services, an independent third party Hotline. There may also be avenues for confidential reporting to the Bank’s Securities Regulators that are discussed in more detail in the *Whistleblower Policy*.
- The Staff Ombuds Office is also available to provide confidential advice or assist you in identifying an appropriate way to report your concerns. (For information on how to contact the Staff Ombuds Office, consult the *Pathways to Resolution* guide or *Key Sources of Guidance and Advice* addendum).

### c. Getting help or advice

You are expected to know and understand this Code, and conduct yourself in accordance with them. If you have any questions or are unsure about any of the principles or requirements of this Code, ask your Manager or a more senior officer. If this is not appropriate, or if you need further guidance, consult the *Key Sources of Guidance and Advice* addendum.

# Glossary

Introduction

Our guiding principles

Principle 1

Principle 2

Principle 3

Principle 4

Principle 5

Principle 6

Getting help or reporting problems and irregularities

## ► Glossary

Key sources of guidance and advice

**Asset** refers to any property of economic value, physical or otherwise, owned by Scotiabank.

**Bank** means The Bank of Nova Scotia.

**Board of Directors** means the Board of Directors of Scotiabank.

**Competition laws** or **trade regulations** generally prohibit or attach specific conditions to arrangements that:

- restrain or monopolize trade;
- have discriminatory price or service features, which diminish competition;
- unduly restrain competition by requiring that the customer deal only, or primarily, in the company's products (sometimes called "exclusive dealing") or that the customer, as a condition of acquiring a specific product, also acquires some other company product (sometimes called "tied selling"); and/or
- represent other methods of competition deemed unfair.

**Compliance Department** means Scotiabank Global Compliance, including Global Compliance Executive Offices (Toronto), and local and subsidiary Compliance departments.

**Confidential business information**, sometimes called "non-public information", is information about Scotiabank or another business that has not been generally disclosed to the public. Confidential business information may include, but is not limited to, financial information, projections, proposed transactions, intellectual property, proprietary processes, trade secrets, and information that might be useful to competitors or information about customers, suppliers, service providers, creditors or shareholders. All information about, or received from, business customers should be presumed to be confidential business information unless the contrary is clear. See also "insider trading".

**Confidential information** comprises customer or employee personal information, confidential business information and any other information about Scotiabank or another business that has not been generally disclosed to the public. See also "personal information" and "confidential business information."

**Conflict of Interest** arises when a person or corporation is in a position to derive personal benefit from actions or decisions made in their official capacity such that the impartiality or objectivity of the person or corporation is undermined.

**Directorship** refers to an elected or appointed position on a company's board of directors.

**Discrimination** means treating people differently, negatively or adversely because of their race, national or ethnic origin, colour, religion, age, sex, gender, sexual orientation, marital status, family status, physical or mental disability or other grounds specifically prohibited in the Canadian Human Rights Act or other human rights and anti-discrimination laws that apply to affiliates, subsidiaries or to Scotiabank's operations globally.

**Employees** means full-time, part-time and temporary, casual or contract employees of Scotiabank. Employees may also include certain independent contractors who, while not technically employees within the meaning of applicable labour or tax laws, have been identified by Compliance as being subject to this Code.

A **fiduciary** is someone who has undertaken to act for the benefit of another and is in a position of trust.

**Information barriers** are the policies, procedures and processes that collectively create barriers restricting access to inside information. This refers in particular to the practice of separating research, sales and trading employees from employees whose jobs make it likely they will encounter inside information.

**Inside information** is material information that has not been generally disclosed to the public. See also "material information".

## Glossary

Introduction

Our guiding principles

Principle 1

Principle 2

Principle 3

Principle 4

Principle 5

Principle 6

Getting help or reporting problems and irregularities

### ► Glossary

Key sources of guidance and advice

**Insider trading** is the legally prohibited activity of purchasing or selling securities of a public company, or derivatives linked to that company's securities, with the knowledge of inside information. See "inside information" and "tipping."

**IIROC** is the Investment Industry Regulatory Organization of Canada, which is the national self-regulatory organization which oversees all investment dealers and trading activity on debt and equity marketplaces in Canada.

**Laws** include any applicable legislation, statutes, regulations, policies, rules and codes of conduct established by governmental, legal or regulatory authority, or by any self-regulatory or industry association by which Scotiabank is or has agreed to be bound.

**Legal Department** means your local or subsidiary Legal Department, or Legal Department Executive Offices (Toronto).

**Manager** means your branch manager, department manager, supervisor or unit head. See also the "Pathways to Resolution" guide.

**Material information** is information which would reasonably be expected to significantly affect the market price or value of a company's securities. It can also be information that an investor would likely consider important in deciding whether to buy or sell a company's securities.

**Money laundering** is defined as the process of concealing the existence, illegal source, or application of income derived from criminal activity, and the subsequent disguising of the source of that income to make it appear legitimate.

**Pathways to Resolution guide** means Scotiabank's published guide, *Pathways to Resolution*. Employees of subsidiaries should read this and words such as "Manager" and "department head" in the context of their organizational structure and escalation processes.

**Personal information** means information about an identifiable individual customer or employee of Scotiabank. This may include, without limitation, the individual's name, address, signature, date of birth, gender, government-issued identification number (e.g. on a driver's permit or passport), income, assets, liabilities, financial account numbers, source of funds, payment records, employee number, personal references and health information. Whether or not credit or other services have been extended, and opinions contained in credit or employee files is also personal information. In general, personal information includes any information that could be used to commit identity theft or other forms of fraud. All information about or received from individual customers or employees should be presumed to be personal information unless the contrary is clear. See also "confidential information".

**Policies, procedures, and processes** refer to all applicable manuals, handbooks, job aids, forms, policies, practices, procedures, processes, standards, programs and requirements as implemented by Scotiabank, including those that relate to how Scotiabank wishes to manage its business in accordance with its business strategy and risk appetite.

**Scotiabank** refers to The Bank of Nova Scotia, all of its subsidiaries, and, where applicable, its affiliates.

**Subsidiaries** means companies owned or controlled in whole or in majority part by Scotiabank.

**Terrorist financing** means using, transferring, transmitting or dealing with funds or property intended to support terrorist activities.

**Tipping** is passing "inside information" about a company to another person, except where the conveyance of the information is in the necessary course of business. See "inside information" and "insider trading".

## Key sources of guidance and advice\*

- Introduction
- Our guiding principles
- Principle 1
- Principle 2
- Principle 3
- Principle 4
- Principle 5
- Principle 6
- Getting help or reporting problems and irregularities
- Glossary

► **Key sources of guidance and advice**

If you have questions or concerns, or wish to report something to a more senior officer within the Bank, use one of the options in the *Pathways to Resolution* guide. If this is not feasible, or if you require additional assistance, consult one of the sources listed below.

Issue	Additional sources of guidance and advice
Accounting and auditing concerns, suspected fraudulent activity and whistleblowing retaliation/retribution	The Chief Auditor or Submit a confidential, anonymous report through the Whistleblower Policy website at <a href="http://www.gcs-whistleblower.com">www.gcs-whistleblower.com</a> (English, French or Spanish language) or Refer to the Whistleblower Policy and Procedures
Criminal activity (known or suspected)	Your designated Security and Investigation Department or Security and Investigation Department (Toronto)
Customer complaint resolution policies or procedures	In Canada: Office of the President 1-877-700-0043 (English) 1-877-700-0044 (French) E-mail: <a href="mailto:mail.president@scotiabank.com">mail.president@scotiabank.com</a> or All others: Your designated Compliance Department
Conflict of interest (Bank insider and corporate client conflicts)	Compliance Control Room (Toronto)
Conflict of interest (other)	Your designated Compliance Department or Global Compliance Executive Offices (Toronto) E-mail: <a href="mailto:business.conduct@scotiabank.com">business.conduct@scotiabank.com</a>

\* Note: Individual business units are encouraged to create and circulate a customized *Key Sources of Guidance and Advice* document using this template.

## Key sources of guidance and advice\*

- Introduction
- Our guiding principles
- Principle 1
- Principle 2
- Principle 3
- Principle 4
- Principle 5
- Principle 6
- Getting help or reporting problems and irregularities
- Glossary

► **Key sources of guidance and advice**

Issue	Additional sources of guidance and advice
Harassment	Employee Relations, through your local Human Resources Call Centre or Your local Human Resources Department
Inside information, information barriers, trading restrictions and insider trading	Compliance Control Room (Toronto)
Legal matters	Your designated Legal Department or Legal Department Executive Offices (Toronto)
Media enquiries	Your designated Public Affairs Department or Public, Corporate and Government Affairs Executive Offices (Toronto)
Money laundering/Terrorist financing (known or suspected)	Your designated Anti-Money Laundering Compliance Officer or Anti-Money Laundering Unit (Toronto) E-mail: <a href="mailto:amlu@scotiabank.com">amlu@scotiabank.com</a>
Off-the-record, confidential advice regarding workplace concerns	Staff Ombuds Office Phone (from Canada and the U.S.): 1-800-565-7810 (English, Spanish) 1-800-565-7804 (French) Phone (International – Call collect during Toronto business hours): 1-416-866-4330 (English, Spanish, French) Email: <a href="mailto:staff.ombudsman@scotiabank.com">staff.ombudsman@scotiabank.com</a>

\* Note: Individual business units are encouraged to create and circulate a customized *Key Sources of Guidance and Advice* document using this template.

## Key sources of guidance and advice\*

- Introduction
- Our guiding principles
- Principle 1
- Principle 2
- Principle 3
- Principle 4
- Principle 5
- Principle 6
- Getting help or reporting problems and irregularities
- Glossary

► **Key sources of guidance and advice**

Issue	Additional sources of guidance and advice
Privacy (customer), including releasing information about customers and breaches of customer privacy	The Canadian Branch Network: Please contact ask.operations@scotiabank.com or 1-844-301-8822 All others: Use one of the options in the Pathways to Resolution guide or contact your designated Compliance Department or Global Compliance Executive Offices (Toronto) E-mail: privacy@scotiabank.com
Privacy (employee), including breaches of employee privacy	Contact your designated Compliance Department or Chief Employee Privacy Officer (Toronto)
Releasing information about Scotiabank	Your manager, supervising office or department head
Safeguarding Scotiabank facilities and assets	Your designated Security and Investigation Department or Security and Investigation Department (Toronto)
Safeguarding electronic information and computer assets	Information Security and Control Executive Offices (Toronto) E-mail: asksecurity@scotiabank.com
Workplace issues or concerns	Contact Employee Relations, through your local Human Resources Call Centre or Your local Human Resources Department

\* Note: Individual business units are encouraged to create and circulate a customized *Key Sources of Guidance and Advice* document using this template.