SCOTIABANK
CODE OF CONDUCT

Scotiabank®

Doing the right thing matters

Dear Scotiabankers,

Trust has been foundational to the relationships we have built with our clients, our shareholders, our fellow Scotiabankers, and the communities in which we operate, for more than 190 years. More than just about meeting our regulatory requirements, trust means acting with integrity and championing a culture where every employee takes ownership of their actions.

We are guardians of our clients' finances—and their futures—and as such, we are held to a higher standard. For Scotiabankers, our goal is not just to win—it is to win the right way, with honesty, with accountability, and in a manner that we can all be proud of.

By signing our Code, you are joining our 90,000-strong team in a promise that we will always do the right thing for all of our stakeholders. Thank you for your commitment to our Code, and for keeping the Bank safe.

Scott Thomson
President & Chief Executive Officer

Contents

A message from our CEO

Doing the right thing matters

Our guiding principles

PRINCIPLE 1

Follow the law wherever Scotiabank does business.

PRINCIPLE 2

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

PRINCIPLE 3

Conduct yourself honestly and with integrity.

PRINCIPLE 4

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

PRINCIPLE 5

Treat everyone fairly, equitably and professionally.

PRINCIPLE 6

Honour our commitments to the communities in which we operate.

Introduction

I. Roles and responsibilities

II. Consequences of failing to comply with our code

III. Scotiabank policies

The *Scotiabank Code of Conduct*[1] (our "**Code**") describes the standards of conduct required of Employees, Contingent Workers, 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 uncertain about what is the most appropriate course of action in a particular situation, this Code should be your first point of reference. As Scotiabankers, if you see something in this Code that you don't understand, or 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 last approved by the Board of Directors on October 18, 2022. The online version of this Code, available at www.scotiabank.com, is the most up-to-date, and supersedes prior versions.

Introduction

I. ROLES AND RESPONSIBILITIES

Over the years, our customers and Employees have trusted us to deliver financial solutions and advice to help them meet their goals for every future. It is this confidence in our Bank, rooted in our Code that has allowed us to develop longstanding and deep relationships that span generations.

New Employees, Contingent Workers, Directors, and officers are given a copy of or link to this Code when they are on-boarded, retained 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 and affirm their compliance within the required timeline on an annual basis. This process is delivered and completed through the annual Code Global Mandatory Learning courses. Ask questions when unclear about your responsibilities or the appropriateness of a particular action, and report any actual, suspected or potential breach of this Code immediately. In addition, all Employees are assigned an accountability goal focused on Keeping the Bank Safe and conducting all activities in line with our Code.

Managers have additional responsibilities to be aware of and communicate applicable Laws, regulatory requirements and internal Policies, Procedures, Guidelines, and Processes, as well as manage and supervise Employees or Contingent Workers 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 or Contingent Workers and ensure that any actual, suspected or potential breach of this Code is dealt with or escalated in accordance with applicable Policies, Procedures, Guidelines, and Processes in a timely manner.

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[2] and must authorize changes[3] to this Code and any waivers[4].

[2] Our Code is formally reviewed, at a minimum, once every two years, or earlier if required.
[3] Notwithstanding the Board of Directors' authority over changes and waivers of this Code, Global 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).
[4] In certain limited situations, Scotiabank may waive application of a provision of this Code to an Employee, Contingent Worker, 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.

Introduction

These roles and responsibilities are summarized in the following chart.

Responsibility	Employee or Contingent Worker	Director	Officer	Manager	Executive Management	Board	Global Compliance	Legal	HR	Information Security & Control	Internal Audit
Read, understand and comply with code and policies	•	•	•	•	•	•					
Affirm compliance	•	•	•	•	•	•					
Ask questions	•	•	•	•	•	•					
Report breaches	•	•	•	•	•		•		•		
Communicate requirements			•	•	•		•		•		
Supervise/Monitor compliance			•	•	•		•	•		•	
Answer questions			•	•	•		•	•	•	•	
Address breaches			•	•	•		•	•	•	•	•
Report on compliance					•		•		•		•
Approve changes to code					•	•	•				
Approve waivers						•	•	•	•		

II. CONSEQUENCES OF FAILING TO COMPLY WITH OUR 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 Employees, Directors, and officers 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 and trust 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, or a Contingent Worker's assignment with, Scotiabank[5] . 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 employment, or in the case of Contingent Workers, termination of assignment or contract. 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.

You should also be familiar with our Code's addendum, *Key Sources of Guidance and Advice.*

III. SCOTIABANK POLICIES

You are expected to be aware of, stay current of, and comply with all applicable Scotiabank Policies, Procedures, Guidelines, and Processes.

[5] For Employees located in the United States, nothing contained in our Code creates or shall be intended to create a contract of employment, express or implied.

Raising concerns

I. Obligation to report

II. Protection from retaliation

III. How to report

Raising concerns

By speaking up and raising concerns, you are helping to ***Keep the Bank Safe*** and protect the trust instilled in us. This section outlines our responsibilities as Scotiabankers and options available to raise a concern.

I. OBLIGATION TO REPORT

You are required to immediately report any actual, suspected or potential breaches of our Code including:

- any actual, suspected or potential breach by you or any other person of a policy, procedure, guideline, law, regulatory requirement, or code of conduct;
- any weakness or deficiency in Scotiabank's Policies, Procedures, Guidelines, and Processes or controls that might enable breaches to occur or go undetected; or
- any failure of a supplier, service provider or contractor to adhere to legal requirements or ethical standards comparable to this Code.

Reporting such matters can help protect you and Scotiabank, as well as other Employees, customers, shareholders and other stakeholders.

Failing to report is grounds for immediate termination of employment for cause, or in the case of Contingent Workers, termination of assignment or contract.

If a problem or concern has been referred to you, resolve the issue or refer it appropriately using one of the options in the *Global Raise a Concern Policy*.

II. PROTECTION FROM RETALIATION

Scotiabank will protect from Retaliation individuals who, in good faith, reports actual, suspected or potential breaches of this Code or violations of law, regulations or internal policies by Employees, Contingent Workers, Directors, officers, service providers, or problems with Scotiabank's Policies, Procedures, Guidelines, Processes or controls.

Retaliatory action of any kind against individuals who makes a report in good faith could be grounds for termination of employment for cause, or in the case of Contingent Workers, termination of assignment or contract, and may be subject to criminal or civil penalties.

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

III. HOW TO REPORT

a. Raise a concern

You should report any actual, suspected or potential breach of this Code to your Manager or as set out in the *Global Raise a Concern Policy*. Consult a more senior officer if you do not receive what you consider to be a reasonable response from the first person. You can also report Harassment or other workplace issues to Employee Relations by contacting Ask HR (in Canada), or to the local Human Resources department or representative.

Actual, suspected or potential 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, you should escalate through alternative options which are available to you.

b. Alternative, confidential avenues

It may not always be appropriate or adequate to report breaches or concerns through *Global Raise a Concern Policy* (for example, if concerned about the possibility of reprisal by persons involved in an actual, potential or suspected breach of this Code). Scotiabank has therefore created alternative, confidential avenues to disclose possible unethical behaviours or Wrongdoing (breaches, problems and irregularities):

- The Staff Ombuds Office is available to provide confidential advice or assist in identifying an appropriate way to report your concerns. (For information on how to contact the Staff Ombuds Office, consult the *Global Raise a Concern Policy* or *Key Sources of Guidance and Advice* addendum).
- The *Whistleblower Policy (Enterprise-wide)* outlines the process for reporting suspected unethical behaviour or Wrongdoing, including reporting accounting and auditing concerns, fraudulent activity or actual, suspected or potential breaches of the law, this Code, a policy or procedure of the Bank, or any voluntary code of conduct or public commitment made by the Bank including concerns related to Retaliation or retribution. The Policy also provides details on avenues for confidential reporting to the Bank's Securities Regulators. The Whistleblower Policy is supported by a third-party portal where anyone can make formal reports online or by phone via a toll-free number. It is accessible 24 hours a day, 7 days a week. The portal can be found at Scotiabank.EthicsPoint.com.

Raising concerns

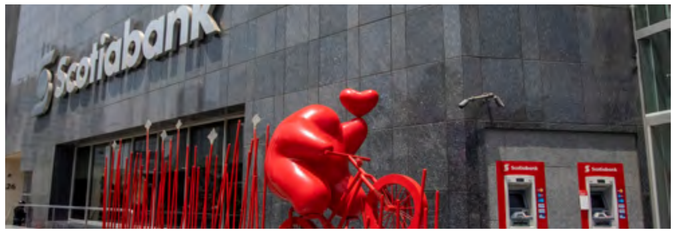
Whistleblower Program - The program provides a confidential mechanism for individuals to confidentially and anonymously come forward and report suspected Wrongdoing. It receives, tracks, and investigates suspected unethical behaviour or Wrongdoing to determine whether such reports are substantiated. The program ensures that Bank management takes steps to remediate and determine root causes of the unethical behaviour or Wrongdoing. Impartial investigations are undertaken on a confidential basis in coordination with key areas across the Bank which are also subject to the confidentiality of the program.

Examples of Reportable Violations

- misrepresentation or falsification of financial statements
- internal Fraud
- improper Sales Conduct or breaches of consumer protection provisions
- insider trading, Commodities Law/Securities violations
- conflicts of Interest
- offering or receiving bribes
- breaches of privacy or confidentiality
- harassment, discrimination and racism
- retaliation or retribution

c. Getting help or advice

You are expected to know and understand this Code and conduct yourself in accordance with our Code and our Code principles. Scotiabankers who have any questions or are unsure about any of the principles or requirements of this Code, should ask their 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.



HOW TO IDENTIFY ETHICAL ISSUES AND HOW TO RAISE A CONCERN

Is the behaviour or activity contrary to our Code principles, and/or breaches Scotiabank policies and procedures?

Is the behaviour or activity in violation of the law and/or regulatory obligations?

Is the behaviour or activity not inconformity with the Bank's Values (Respect,Accountability, Passion, Integrity)?

Does the behaviour or activity have the potential to adversely impact customers, employees, and/or the financial markets?

Does the behaviour or activity have the potential to negatively impact the Bank's reputation or brand, the trust instilled in us, or our ability to keep the Bank safe?

Is the behaviour or activity likely to negatively impact your good reputation if it were made public?

If you answered "yes" to any of these questions, you need to Speak Up and Raise a Concern. Your Raise a Concern Channels include:

- Speaking to your manager, or other senior leader
- Staff Ombuds Office
- Ask HR / Local HR (Canada) or your Local HR Representative (all other locations)
- Whistleblower Program.

Our guiding principles

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.

PRINCIPLE 1

Follow the law wherever Scotiabank does business.

PRINCIPLE 2

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

PRINCIPLE 3

Conduct yourself honestly and with integrity.

PRINCIPLE 4

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

PRINCIPLE 5

Treat everyone fairly, equitably and professionally.

PRINCIPLE 6

Honour our commitments to the communities in which we operate.

Principle 1

Follow the law wherever Scotiabank does business.

I. Your responsibilities

II. Conflicting requirements

Principle 1

Follow the law wherever Scotiabank does business.

Advice that can put Scotiabank at risk:

Scotiabankers 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.

I. YOUR RESPONSIBILITIES

Ask Questions… Comply… Report!

Scotiabank is expected to comply with the Laws that govern our business activities. There are legal 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, Procedures, Guidelines, and Processes 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. You are expected to know the Policies, Procedures, Guidelines, and Processes that are relevant to your activities, act in accordance with the letter and spirit of these Policies, Procedures, and Guidelines, and Processes, 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. *What* we achieve as a business is important, but how we get there matters just as much.

Scotiabankers who are unclear about legal, regulatory or other requirements should consult their Manager. If necessary, you can seek the advice of the Compliance Department, Legal Department, Information Security & Control (IS&C) or the Bank's Data Protection Program (DPP).

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

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 *Global Raise a Concern Policy* or using the other avenues described in the section *Getting Help and Reporting Problems and Irregularities* at the end of this Code.

II. CONFLICTING REQUIREMENTS

In the case of any conflict between the provisions of this Code and any Laws, regulatory requirements or any other Policies, Procedures, Guidelines, or Processes applicable to your position, or a Contingent Worker's assignment with the Bank, you must adhere to the more stringent requirement.

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, you must consult with the Compliance Department and keep a written record of such enquiries and responses.

Principle 2

Avoid putting yourself or Scotiabank in a conflict of interest position

I. Personal conflicts of interest

II. Corporate conflicts of interest

Principle 2

Avoid putting yourself or Scotiabank in a conflict of interest position

I. PERSONAL CONFLICTS OF INTEREST

You 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.

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 and impartially. 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.

As a Scotiabanker, 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 disclose to your Manager so that appropriate action can be taken to resolve the situation. This is the best way to protect yourself and your reputation for honesty, fairness, integrity 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 common conflicts that may arise and provides 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 their will.	The customer's family, or others, may perceive that the Employee used their position to unfairly coerce, manipulate or take advantage of the customer.
An Employee accepts a gift of tickets for themselves and their family to an expensive, sold-out sports event from a customer.	The Employee risks a perception by others that they could be improperly influenced in their judgment when making lending or other decisions related to the customer's 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.
A manager has an immediate family member as a direct or indirect report (family members include, siblings, parents, grandparents, children (including step-children and adopted children) and grandchildren, spouse or common-law spouse, and in-laws).	Other Employees and third parties may perceive a conflict of interest and/or favoritism. Our business and human resources decisions must be based on sound ethical business and management practices, and not influenced by personal concerns.

Principle 2

Avoid putting yourself or Scotiabank in a conflict of interest position

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

As a Scotiabanker, when you deal with the Bank 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[6]. This means that Scotiabankers may only transact business, make entries or access information on their own accounts using the same systems and facilities available to non-Employee customers. For example, you can use the ABM or online or mobile banking to transfer funds between your own accounts, since this service is generally available to non-Employee customers. Do not use internal platforms, applications, or systems to access your own personal customer profiles and accounts.

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. For example, Scotiabankers must not set up accounts for themselves, or on behalf of these individuals, without the review and agreement of their 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). Do not use internal platforms, applications, or systems to access their customer profile without such documented authorization.

Under no circumstances may a Scotiabanker authorize or renew a loan, or lending or margin limit increase to themselves, a family member, a friend or other close associate. As a Scotiabanker, you may not 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. Close personal relationships in the workplace[7]

Conflicts of interest (or the appearance of a Conflict of Interest) can arise when Scotiabankers work with those with whom they share a close personal relationship (such as family relationships, romantic relationships and/or financial relationships[8]) and can also raise serious concerns about favouritism and, in the case of certain close personal relationships, the validity of consent.

In accordance with the *Global Close Personal Relationships in the Workplace Policy*, Scotiabankers must immediately disclose potential or actual conflicts of interest related to close personal relationships in the workplace to their manager, or follow the process in the *Global Raise a Concern Policy* and *Examples of Workplace Concerns Guide*, so that appropriate action can be taken.

c. 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.

d. Outside business activities, financial interests or employment

For Employees, having other work (paid or unpaid) outside of your employment with Scotiabank 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:

- Do not engage in work that competes with Scotiabank, or in any activity likely to compromise or potentially harm Scotiabank's position or reputation.
- Participation in an outside business activity should only be conducted outside of normal working hours and not use Scotiabank Confidential Information (including information about Scotiabank, Employees and customers) or Scotiabank equipment or facilities. This includes soliciting other Employees or Scotiabank customers to participate in an outside business activity.
- Employees owe a duty to Scotiabank to advance its legitimate interests when the opportunity to do so arises, and may not take for themselves a business opportunity that is discovered in the course of Scotiabank employment or assignment, or through the use of Scotiabank property, information (including information about Scotiabank Employees, vendors/suppliers, or customers), or your position.
- Neither Employees nor members of their 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 give rise to a Conflict of Interest.[9]

[6] Note: This is subject to any special policies or procedures that may be applicable to individuals in certain job functions, business units or Subsidiaries.
[7] Please refer to Footnote 6 above.
[8] For example, having obligations as a power of attorney, an executor, a trading authority, a business partner in outside business activities etc.
[9] 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, including the *Scotiabank Personal Trading Policy*.

Principle 2

Avoid putting yourself or Scotiabank in a conflict of interest position

- Employees should seek approval from their Manager (or department head, where appropriate) prior to taking on an outside business interest or committing to a job outside of normal working hours. The Employee's Manager (or department head, where appropriate) is responsible for reviewing the circumstances of the outside business and ensuring that these activities do not create a Conflict of Interest. If the Manager (and/or department head) is comfortable there is no real or perceived Conflict of Interest, they are responsible for approving the activity as appropriate. If the Manager has any questions regarding whether there may be a real or perceived Conflict of Interest, they should consult the Compliance Department.

Local regulatory requirements, including securities legislation, or local compliance policies may impose further restrictions on engaging in outside business activities by requiring:

- prior disclosure;
- prior approval by the Bank;
- notice to applicable local regulator; and/or
- approval by applicable local regulator

Please refer to local business line compliance policies and the *Outside Business Activities Guidelines* for further information.

Any questions regarding outside business activities should be discussed with your Manager and/or your Business Line Compliance Department to be sure the proposed outside business activities do not create a conflict.

SAMPLE OUTSIDE BUSINESS ACTIVITIES

SITUATION	POTENTIAL CONFLICT
An Employee is a financial advisor in a branch who recommends mortgages for Bank customers while also working as a real estate agent during the weekend.	Employee can personally benefit from selling real estate by soliciting Bank customers while also arranging the financing, giving rise to both real and perceived conflicts of interest.
An Employee has an online business selling hand-made artwork and solicits Bank customers and Employees. In addition, the Employee takes client calls for the outside business during normal working hours at the Bank.	Employees should act in the best interests of the Bank and cannot use Bank resources and/or time to take part in or solicit business for outside business activities for personal gain.
An Employee was nominated to join as a board member of a non-profit organization which was a customer of the Bank. The Employee also managed the relationship between the Bank and the entity	Conflicts would arise between the interests of both the Bank and the organization. The Employee must disclose the relationship to both the Bank and the board of the organization, they should also remove themselves from any discussions (within the Bank and/or the organization) regarding financial dealings between the Bank and the organization.

e. Misuse of confidential information

You are regularly entrusted with Confidential Information that is not or may not be publicly known about Scotiabank, its customers and fellow Employees or others. This information is provided strictly for business purposes. It is wrong, and in some cases illegal, for anyone to access Confidential Information without a valid business reason to do so, or to use Confidential Information in order to obtain a personal benefit or further their own personal interests. It is also wrong to disclose Confidential Information to any other person or third party who does not require the information to carry out their job responsibilities on behalf of Scotiabank and who is not authorized to access such Confidential Information.

Principle 2

Avoid putting yourself or Scotiabank in a conflict of interest position

f. Directorships

Obtaining Approval: Employees or officers may not accept a corporate Directorship until obtaining approval from their Manager and the Compliance Department.[10] The Compliance Department will seek any other necessary approvals pursuant to the *Scotiabank Corporate Directorships Policy*. New Employees must immediately report any Directorships in accordance with these requirements and seek approval where necessary. If you change your role within Scotiabank, you must advise your new Manager of any Directorships, even if the Directorship was previously approved. Your new Manager can decide, based on the new role, whether the prior approval must be reconfirmed.

Directorships of public companies are prohibited. Exceptions require the approval of the President and 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 Directorship(s) that it determines poses 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):[11]

- non-profit, public service corporations such as religious, educational, cultural, recreational, social welfare, philanthropic or charitable institutions or residential condominium corporations;
- family-owned corporations whose sole purpose is to own the home in which the Employee resides;
- directorship roles in residential condominium corporations; and
- private, family-owned corporations incorporated solely 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 (includes spouses, parents, spouse's parents, children, grandchildren, spouses of children or grandchildren, and relatives with disabilities). This does not include Directorships in for-profit corporations owned by Employees and/or other members of the Employee's family.

However, approval will be needed for certain Employees that are registered with or licensed by certain regulatory authorities (e.g. securities regulators). The Bank or regulatory authorities may attach specific conditions to any approval to address concerns including the management of potential conflicts of interest.

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

g. Wills, other trusteeships and similar appointments

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

Employees should never solicit from, nor accept a personal appointment by, a customer as an executor, administrator or trustee, with some exceptions made for family relationships.

If Employees 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. Management approval will be required for signing authority for the estate's bank accounts. (Some affiliates and Subsidiaries may require additional approvals.)

h. Purchasing/Selling Scotiabank assets

To avoid the appearance that Scotiabank is giving an advantage, you or members of your household may not purchase Scotiabank Assets such as automobiles, office equipment or Computer Systems, 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 the appropriate business unit head has approved the transaction; or
- the purchase is made under an approved Scotiabank program.

Unless it's part of your job, and under an authorized Scotiabank program, you may not sell Scotiabank Assets. It is also strictly prohibited to advertise or sell any Bank asset for personal gain or to further your own interests.

[10] 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, Guidelines and Processes.
[11] While preapproval is not required, Employees at or above the level of Vice President are required to report these directorships to the Compliance Department

Principle 2

Avoid putting yourself or Scotiabank in a conflict of interest position

i. Administered or repossessed property

Neither you nor your family may use or purchase goods that have been repossessed by Scotiabank, except with the permission of the appropriate Group or Country Head, who will review the situation and consider whether the transaction would both be, and appear to be, fair.[12]

j. 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.

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;
- Scotiabank's relationships with one third party supplier could conflict with its obligations to another third party supplier.

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 financing for more than one customer's bid for the same asset.	Risk of being perceived to have improved Scotiabank's position at the expense of a customer.
Scotiabank is asked to provide third party financial information to another third party for benchmarking purposes.	Risk of breach of confidentiality owed to third parties and risk of being perceived as having improved Scotiabank's position at the expense of a third party supplier.

Employees, including lending or advisory officers must be alert to situations where there may be a conflict or the appearance of one. Those who become aware of a potential conflict must observe Policies, Procedures, Guidelines, and Processes regarding confidentiality and Conflicts of Interest and advise their 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* and the *Scotiabank Global Anti-Bribery & Anti-Corruption 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.

[12] Those who work for a securities subsidiary, or any other subsidiary or area where a Fiduciary obligation may be imposed by law, may not use, or become the owner of, property held in Fiduciary accounts under administration, unless they or a family member are a beneficiary or co-trustee of an estate and the governing document specifically permits use, or ownership of, the property being administered.

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 3

Conduct yourself honestly and with integrity

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 may be grounds for termination of employment for cause, or in the case of Contingent Workers termination of assignment or contract, and possible civil or criminal liability. This includes, but is not limited to, falsely inflating or mis-representing performance results to gain additional compensation, falsifying expense claims, misuse of Employee benefits such as corporate credit cards or Employee banking privileges (including purchasing foreign currency for anyone other than eligible dependents) or medical/dental benefits, or manipulating Scotiabank's clearing or payments systems (including but not limited to cheque writing and any ABM, online or mobile banking transactions) or General Ledger accounts to obtain credit or funds fraudulently.

You are also stewards of Scotiabank's resources and must act in the Bank's, and ultimately the shareholders' interests by spending the Bank's money responsibly. Scotiabank's expense policies and procedures governing authorization and reimbursement of reasonable employment expenses must be adhered to.

b. Improperly accessing records, funds or facilities

Never use your Scotiabank access to funds, facilities or systems 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.

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, including family members, 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 privacy breach and a breach of this Code and may subject you to discipline, up to and including termination of employment or, in the case of Contingent Workers, termination of assignment or contract.

You may not access or use Scotiabank facilities on behalf of third parties. In addition, any personal use must be limited to Reasonable and Occasional Personal Use. For example, the use of Scotiabank mailroom facilities to receive personal postal mail.

You may not 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

Creating false records is a breach of the law and this Code and could result in termination of employment or assignment/contract in the case of Contingent Workers and or legal proceedings against you by Scotiabank and the affected individuals.

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.

Knowingly making or allowing false or misleading entries to be made to any Scotiabank account, record, model, system or document is a crime of Fraud and a serious violation of this Code (this includes, but is not limited to, inflating sales numbers to receive higher commissions, falsifying sales that did not occur or colluding with customers or other Employees to record and collect commissions on falsified sales).

In addition, undisclosed or unrecorded Scotiabank accounts, funds, Assets or liabilities are strictly prohibited. Immediately report your knowledge or discovery of any such account, instrument or misleading or false entry as described by the Whistleblower Policy (Enterprise-wide), which is one of the options in the *Global Raise a Concern Policy*.

d. Bribes, payoffs and other corrupt practices

Scotiabank prohibits offering, or accepting, directly or through an intermediary, kickbacks, extraordinary commissions, facilitation payments, or any other improper kind of payment or benefit or anything of value to or from suppliers or service providers, customers, public officials, Politically Exposed Persons ("PEP")[13] or others in exchange for favourable treatment or consideration.

[13] For complete definition of public officials and Politically Exposed Persons, please refer to the *Scotiabank Global Anti-Bribery & Anti-Corruption Policy*

Principle 3

Conduct yourself honestly and with integrity

Accepting money, gifts, or anything of value from actual or potential intermediaries/business partners, such as dealers, lawyers, consultants, brokers, other professionals, suppliers and service providers in exchange for selecting them to provide services is prohibited. Intermediaries/business partners should be selected on the basis of qualifications, product or service quality, price and benefit to Scotiabank, and in accordance with the *Scotiabank Global Anti-Bribery & Anti-Corruption Policy* and procedures.

For additional guidance on Scotiabank's policies with respect to the prevention of bribery and corruption and how to escalate concerns, refer to the the *Scotiabank Global Anti-Bribery & Anti-Corruption Policy*. You may also contact Conduct.Risk@scotiabank.com for further advice or guidance.

e. Insider trading and tipping

In the course of your duties, you may become aware of Confidential Information about Scotiabank or another public company. Some 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 would be reasonable to expect that the price of the securities could be significantly affected. This kind of information is commonly called Inside Information and you may not act on this information for your, or a close friend or relative's benefit (this is known as Insider Trading).

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 conducting Scotiabank business. This activity is commonly called Tipping.

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.

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.[14]

If you are likely to encounter Inside Information you should become familiar with the specific policies and procedures that Scotiabankand 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

You are prohibited under provisions of the Bank Act from trading in calls or puts (i.e. options to buy or sell securities at a set price) on Scotiabank securities.

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

g. Requirement to disclose a criminal charge or conviction for which a pardon has not been granted

You are required to disclose to Scotiabank if you are charged with, or convicted of, any criminal offence in a domestic, foreign or military jurisdiction or court. If you are charged with or convicted of any criminal 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. You must also update the Bank on any developments relating to charge or conviction.

h. Anti-Competitive Practices

To promote fair and open competition among businesses in similar industries, many countries have competition and anti-trust laws. As such, you should be familiar with the *Scotiabank Competition Law Compliance Policy*.

Do not collude or co-operate with any other competitor in anti-competitive activities, including arrangements or agreements to:

- Fix the price of products or services (including interest rates on loans and deposits, fees, rates on key indices);
- Divide or allocate customers or geographic areas;
- Restrict the supply of products or services in the market;
- Engage in bid rigging (e.g. agree on how to respond to a tender);

[14] Where permitted by the Compliance Department, sales and trading staff may continue to accept unsolicited orders from customers.

Principle 3

Conduct yourself honestly and with integrity

- Provide or receive competitively sensitive information; and
- Other anti-competitive activities, including tied selling, abuse of dominance or deceptive marketing practices.

You may participate in industry associations or events, but these meetings must not be used to engage in anti-competitive activities.

If you have any concerns about whether an activity or discussion with competitors would violate competition and anti-trust laws, you must refrain from participating and consult with the Legal Department or Compliance Department.

II. IMPROPER TRANSACTION PREVENTION

a. Know Your Customer

Knowing your customer forms the foundation of the financial services industry. Knowing your customers helps to better serve their needs, meet regulatory requirements, avoid facilitating activity that is outside of our risk appetite (including that which could potentially harm Scotiabank's reputation) 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 customer 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 or regulation. Follow designated policies and procedures for transactions that, by Scotiabank's standards, could be considered improper or suspect.

b. Detecting and reporting suspicious or improper transactions

Money Laundering, Terrorist Financing, violation of economic sanctions, tax evasion and acts of corruption committed by customers are serious international problems that receive significant attention as nations attempt to deal with the harmful legal, economic, and social consequences of illegal activities. You should familiarize yourself with the Policies, Procedures, Guidelines, and Processes related to anti-money laundering, anti-terrorist financing, anti-bribery & anti-corruption, and compliance with sanctions that are applicable to your role. Be alert to any illegal, suspicious or unusual activity, including fraud, Money Laundering, Terrorist Financing or breach of government-imposed sanctions requirements.

Scotiabankers must promptly report any unusual account activity to their Manager or, in the case of suspected Money Laundering, Terrorist Financing or sanctions breaches, their designated Anti-Money Laundering Compliance Officer/Local Sanctions Officer. Failure to report a transaction for which there are reasonable grounds to suspect is associated with Money Laundering, Terrorist Financing or a sanctions breach, may be viewed as 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 or will be made about them or their activities.

III. ETHICAL BUSINESS PRACTICES

a. Offering and Accepting Gifts and Entertainment

Customers and business associates often try to show their appreciation by providing gifts and entertainment. Similarly, you may wish to show your appreciation to our customers and suppliers by offering gifts and entertainment. Offering or accepting gifts or entertainment 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.

Subject to the special considerations discussed below relating to government officials, public office holders ("public officials") and PEPs, examples of the types of gifts and entertainment 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;
- modest honoraria and reimbursement for reasonable expenses (if not paid by Scotiabank) for Scotiabank-related speaking engagements or written presentations; or
- gifts or entertainment clearly motivated by obvious family or close personal relationships, rather than business dealings.

Where the monetary value of an item is not nominal or modest in nature, you should consult with your Manager regarding the appropriateness of the gesture. Your Manager should consult with the Compliance Department for guidance on difficult situations.

Principle 3

Conduct yourself honestly and with integrity

In general, the giving and accepting of gifts and entertainment is only permitted if:

- the gift or entertainment is modest[15] and would not affect the recipient's objectivity;
- there is no suggestion that the offeror 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;
- it is not a gift or prize of cash or cash equivalents, bonds or negotiable securities, personal loans, or other valuable items (such as airline tickets for your personal use, or use of a vacation property); although store or vendor specific gift certificates or gift cards are allowed as long as their intended purpose is for the purchase of what would otherwise be considered a gift and is nominal in value.

Remember the following when considering whether to **accept** a gift or entertainment:

- 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.
- Where it would be extraordinarily impolite or otherwise inappropriate to refuse a gift of obvious value (i.e. exceeding what would be reasonably considered nominal value), you may accept it on behalf of Scotiabank. In these cases, they must immediately report the gift to their Manager, who will advise proper action to take. Such gifts may not be taken for personal use or enjoyment.

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

- Always exercise caution and never give, offer, accept or agree to receive a gift, or entertainment during or immediately before or after entering into negotiations on behalf of the Bank, or while awaiting or awarding a contract renewal as the timing may imply that the gift, or entertainment has been provided or promised to influence the recipient. All gift and entertainment expenses must be properly documented and accurately and fairly recorded. Proper documentation should include at a minimum:
  - supporting invoices and receipts
  - name of the person or organization providing and receiving the gift or entertainment
  - legitimate business reason for the expense in sufficient and accurate detail
  - appropriate approvals for the expense
- Be especially careful when offering gifts or entertainment to public officials or PEPs as many countries have strict Laws regarding offering anything of value to these individuals or to third parties at their request. Please also refer to the *Scotiabank Global Gifts and Entertainment Policy* and specific Gifts and Entertainment Operating Procedures within your business unit relating to the offering of gifts and entertainment.
- Always comply with the *Scotiabank Global Anti-Bribery & Anti-Corruption Policy, the Scotiabank Global Gifts and Entertainment Policy* and specific Gifts and Entertainment Operating Procedures in any dealings with public officials or PEPs. Gifts exceeding CDN$125 or US$100 (for US entities only) to or from public officials or PEPs are not permitted. Gifts, Hospitality or Entertainment expenses to public officials or PEPs will require prior approvals as set out in the *Scotiabank Global Gifts and Entertainment Policy* and Gifts and Entertainment Operating Procedures applicable to the relevant business unit or corporate and support function.

For additional information on acceptable gifts and entertainment, consult the *Scotiabank Global Gifts and Entertainment Policy* and specific Gifts and Entertainment Operating Procedures applicable to your business unit or corporate and support function.

b. Charitable donations or sponsorships

Customers and business associates often try to show their appreciation by making charitable donations on your behalf to a charity or through sponsorships. Similarly, you may wish to show your appreciation to our customers and suppliers by making charitable donations to a charity on behalf of, or through sponsorship of, a customer or business associate. Offering charitable donations or sponsorships can be problematic because it may:

- create the appearance of improper influence or a quid pro quo arrangement;
- be perceived as the offer or acceptance of a bribe and/or kickback;
- violate legal and regulatory obligations; and
- harm Scotiabank's position or reputation.

[15] Through the *Scotiabank Global Gifts and Entertainment Policy* and applicable Gifts and Entertainment Operating Procedures, a business unit may set specific acceptable limits or amounts regarding permitted gifts and entertainment.

Principle 3

Conduct yourself honestly and with integrity

In general, making charitable donations or sponsorships is only permitted if:

- the donation or sponsorship is modest or nominal 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 a donation or sponsorship 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 donation or sponsorship;

Remember the following when considering a donation to a charity on your behalf or through sponsoring you:

- 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.

Be especially careful when making charitable donations on a public official's or PEP's behalf or at his or her request as this may be perceived as a bribe. In addition, many countries have strict Laws regarding offering anything of value to these individuals or to third parties at their request.

c. 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. It is important to reiterate that *what* we achieve as a business is important, but *how* we get there matters just as much.

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.

Scotiabankers who discover misrepresentations or misstatements in information provided to customers or the public must consult their Manager about how to correct those statements.

All applicants for employment at any level within Scotiabank must be considered based on appropriate qualification, and compensation must be appropriate for the work being performed and consistent with the compensation paid to other Employees for similar work. Never give preferential treatment, including hiring, retaining, promoting, or in respect of compensation, to individuals based on personal relationships, or family, political, governmental or other affiliations. The employment of a public official or a PEP, or a family member or close associate of a public official or PEP, 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 or PEPs (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 close associate of an official could be perceived.

Furthermore, never engage in behaviour that threatens, pressures, constrains, or otherwise influences an individual to act inappropriately, against their will, and/or in violation of Scotiabank policies.

Never seek to obtain personal advantages from Scotiabank customers or other business relationships.

For example, as a Scotiabanker you must 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[16], 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 to designated groups of Employees.

Also, never access, collect, disclose or use Confidential Information or proprietary information obtained from third parties, other organizations or former employers for the benefit of Scotiabank without proper authorization.

Coercive Tied Selling:

Never pressure customers to buy a product or service that they do not want as a condition for obtaining another product or service from Scotiabank. (This practice, which is illegal in most 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.

[16] 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.

Principle 3

Conduct yourself honestly and with integrity

d. Respect Intellectual Property Rights

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

Only authorized and registered software and hardware are permitted for use within Scotiabank or for use in respect of any Bank business activities. Scotiabankers may not download any third-party intellectual property including software, creative works or other materials; if doing so would violate any vendor/owner rights. Be aware that software or services available over the Internet, including free and demo software or cloud-based services, 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, programs and content, comply with the licensing, confidentiality and registration requirements. For example, do not share registration or access information for external databases or online publications with others as this could be a breach of the licensing and copyright subscription terms or could 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, and the guidance on respecting intellectual property Laws set out within.

As Scotiabankers, 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.

e. Data Ethics

We do not compromise our ethics for the sake of profits or meeting other targets, and the same goes for the use of our customers' data. Scotiabank collects and creates data, which it relies on for data-driven business decisions. This should be done to deliver the best banking experience to our customers and with their interests in mind. In order to do that, and to maintain our customers' trust, Scotiabank has a set of data ethics principles to guide the use of data in supporting the Bank's activities. These principles help data practitioners ensure their decisions include ethical considerations and promotes accountability to align to with our ethical principles throughout the data lifecycle – from when data is acquired, managed, analyzed, used, shared, and eventually disposed. Integrating these principles into the everyday activities of the Bank helps put our customers first by strengthening ethical decision-making processes and ensuring a culture of data ethics.

Our data ethics principles articulate that our use of data is:

1. Useful
2. Adaptable
3. Accountable
4. Transparent
5. Respectful
6. Safe

IV. ENGAGING THIRD PARTIES

In conducting business, Scotiabank uses suppliers or service providers and contractors and may enter into a variety of products and services agreements, outsourcing arrangements or other strategic alliances. If you are authorized to engage third parties, you must do so in compliance with the *Global Procurement Policy* as well as Third Party Risk Management requirements and should engage only those who are competent and reputable, and who have business conduct standards comparable to our own. Service providers, vendors and other third parties providing goods and services to Scotiabank should always follow Scotiabank's Supplier Code of Conduct. Engaging family or household members, or any other person or entity you have a close personal relationship with, 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, regulators, or other Employees by making false or misleading statements or by withholding information.

a. Advertising

Scotiabank is subject to regulations with respect to advertising, which include any written or verbal representations about Scotiabank products and services that are directed at the general public (e.g., social media, online, telephone, email). In general, advertisements must be accurate, clear and not misleading. This includes representations by third parties made on behalf of Scotiabank (such as influencers and paid

Principle 3

Conduct yourself honestly and with integrity

partners). Ensure that established approval procedures are followed or get managerial approval or approval from a department head before initiating any advertisements or representations.

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*. Unless it is part of your job responsibilities, refer inquiries from the financial community, shareholders and media to Global Communications.

c. Making public statements and media contact

Unless authorized to speak to reporters or the media on behalf of Scotiabank, refer all media enquiries to Global Communications. Be especially careful never to respond to questions about a matter where litigation is involved, regardless if it is pending, in progress or resolved (without prior authorization of the Legal Department) and always respect Scotiabank's duty of confidentiality to its customers, Employees and others.

Sometimes Scotiabankers may be asked to give presentations or express views on matters generally relating to banking or other financial services. Speaking opportunities at conferences and industry events should be treated as public events where media may be in attendance or people may share the information presented to social media platforms. Scotiabankers must ensure that their Manager provides approval for any public speaking events they are asked to participate. 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. Should you be unclear on the appropriateness of the content of your presentation, please engage Global Communications.

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 Global Communications.

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, logos, 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, Corporate Security, Information Security & Control, Fraud Management or Human Resource Departments. Be straightforward 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. For more information, refer to the *Enterprise Records Management Policy*.

Principle 4

Respect privacy, 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 4

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

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 *Scotiabank Privacy Agreement*, *Employee Privacy Policy*, and *Scotiabank Incident and Breach Management Procedures*. 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 or others (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 or others' Personal Information (such as to a customer's family member) could be a privacy breach and a breach of this Code and can have serious consequences for you, Scotiabank and the customers involved.

Appropriate handling of personal and Confidential Information includes the following:

- Follow Policies, Procedures, Guidelines, and Processes for storing, handling, and controlling access to electronic and physical Confidential Information.
- Follow any Policies, Procedures, Guidelines, or Processes for transmitting Confidential Information. Do not send Confidential Information via non-secure media such as fax, personal email, SMS/text, instant messaging, web and mobile applications or the Internet (this includes internal and external social media platforms). Follow the Scotiabank Secure Email Service 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 includes also when working remotely).
- Do not disclose Confidential Information to persons outside Scotiabank (including family or household members or close associates) or to others 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 or by smart assistant devices. 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.

Never access customer or Employee or other individual's Personal Information (including your own file), or confidential business information about Scotiabank or a customer, without a legitimate business reason and appropriate authorization. "Snooping" into files of customers or other Employees or others is prohibited. For example, do not view customer profiles or account information of family members, friends or acquaintances without a valid business reason to do so. Snooping is a breach of the law and this Code, and could result in discipline, up to and including, termination of employment or, in the case of Contingent Workers, termination of assignment or contract, and legal proceedings against you by Scotiabank and the affected individuals.

Accessing, collecting and/or using Confidential Information from other organizations, including a former employer, is prohibited.

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

Principle 4

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

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 or potential breach of privacy or confidentiality immediately report it to your Manager or through one of the options described in the *Key Sources of Guidance and Advice* addendum to this Code *or* in the *Raise a Concern How-to-Guide* so that steps can be taken to prevent, minimize or mitigate any negative impact on customers, Employees, other stakeholders, 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, assistance from the Legal Department may be required to verify if a demand for information has been properly made and documented to permit or compel production of information under the law without customer consent.

There may also be situations where legal requirements prohibit telling the customer about a demand for information.

Never access customer or Employee or other Confidential Information without a legitimate business reason and appropriate authorization. "Snooping" into files of customers or Employees or others is a privacy breach, a breach of the law and this Code, and could result in discipline, up to and including, termination or, in the case of Contingent Workers termination of assignment or contract, and legal proceedings.

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. Everyone must play their part in ensuring the accuracy and integrity of our record-keeping and information reporting systems. Follow applicable Policies, Procedures, Guidelines, 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, or feel pressured to do so in order to meet targets, immediately report the incident using one of the options in the *Global Raise a Concern Policy*.

Should you find or notice any weaknesses, deficiencies or inconsistencies amongst any procedure or policy, immediately report your findings to your manager or an appropriate senior officer (e.g. the owner of the policy or procedure).

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, other communication channels, 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.

Principle 4

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

Be careful not to compromise security through the inappropriate or unintended disclosure of information or images (e.g. posting pictures that contain Scotiabank information, taking a photograph with a whiteboard in the background). 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 access/use a public cloud service from a Scotiabank Computer System or device or to conduct any Bank business, unless the service has been approved by the designated committee (Enterprise Architecture Review Board). Never copy Bank files or data to Internet storage services (e.g. Google Drive, DropBox) unless the service has been approved by the Bank's governance forums.

Use only approved communication channels on Bank approved devices to conduct Scotiabank business. Use of unauthorized communication channels for business communications is considered a breach of our Code.

For further information on approved communication channels, please refer to the *Global Voice and Electronic Communications Policy*.

Report any perceived weakness or deficiency in a system or a 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, systems and software, and communication channels; 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

As Scotiabankers who 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 Risk and Control Assessment has been conducted with the assistance of Information Security & Control.

d. Use of Scotiabank property and information when working remotely/offsite

As Scotiabankers when you are working 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, Guidelines, and Processes; and
- never copy Scotiabank information for your or someone else's non-work-related use without authorization.

Scotiabankers are required to follow the standards noted below when working remotely or from home:

- take reasonable steps to set up a workspace in a private area;
- secure the designated workspace when it is left unattended. Lock down all unattended equipment and shut down completely at the end of your workday;
- use only Bank-issued device(s) for all business activities and avoid using personal devices in any circumstances including sending business information to personal emails to print documents;
- do not use printers at home to print Bank documents without proper authorization;
- properly secure all proprietary information to prevent unauthorized access;
- be vigilant with smart assistant devices (e.g., Google Home, Amazon Alexa, etc.), and ensure they are not in listening range of business conversations;
- take appropriate precautions to maintain confidentiality should you live with a Bank customer, or someone who works at a competitor bank or supplier;
- be mindful that conversations regarding confidential information should be out of earshot, i.e., that other people should not be able to hear them. Always use code names and project names during business conversations where applicable; and

Principle 4

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

- do not take pictures of your dedicated workspace when working remotely while monitors display Bank information or Bank documents.

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

e. Appropriate use of information technology and services

As Scotiabankers, appropriate use of information technology and services, electronic and telecommunications facilities and systems, such as computers, Internet access, voice mail, e mail, fax machine, scanners and telephone, are provided to you to enable you to do your job. Any other use, except for Reasonable and Occasional Personal Use, is not allowed.

Additional responsibilities expected from Scotiabankers include the following:

- advise Scotiabank if your Bank-issued device, such as your laptop or phone, is lost or stolen as soon as is reasonably practical to do so;
- ensure proper technical updates/patches (e.g. operating system and application updates) have been completed in a reasonably timely manner when made available or required.

Scotiabank monitors for appropriate access to and use of information technology services and physical storage facilities in order to prevent and detect improper access to, and use of, information.

- do not interfere or attempt to interfere with the security settings or the system configuration of any Bank owned or provided computing devices including mobile devices and computer systems (e.g., “jailbreaking” or “rooting”);
- work-related files are not to be stored on personally acquired storage/sharing services (e.g., Apple iCloud, Dropbox or Google Docs);
- personally acquired webmail services (e.g. Gmail, Yahoo Mail, Hotmail) are not to be used for work related emails. This includes communication, scheduling and storage of attachments;
- work-related photos or scanned images are not to be stored/shared on personally acquired photo storage/sharing services (e.g. Picture Frame, Photostream);
- personally acquired cloud-based data-processing or voice processing services are not to be used for business purposes (e.g. use Scotiabank PROMT Translation - translate.bns); and
- use only applications provided through Scotiabank Information Technology and Solutions when conducting Scotiabank business.

IV. DIGITAL COMMUNICATIONS, USE AND REPRESENTATION

Inappropriate Internet use outside the workplace could subject you or Scotiabank or its customers or other stakeholders 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’). You should also be aware of and comply with all applicable policies or procedures with respect to the sending of emails and other 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 names or other proprietary materials without prior approval. If approved, ensure that you follow the branding guidelines of Scotiabank, Subsidiaries or business line 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 internal or Confidential Information – including information about customers, Employees, others, or Scotiabank – be posted online. This includes information on Scotiabank’s security procedures, practices or vulnerabilities, as well as images or representations of Scotiabank facilities;
- do not post or otherwise disclose the Confidential Information of customers, Employees or Scotiabank; and

Principle 4

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

- be alert for fraudulent activities and social engineering techniques. Social engineering is a collection of techniques, including phishing, used to trick you into divulging confidential personal or business information or granting access to secure systems. If you become aware of fraudulent activity, notify Corporate Security.

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, Guidelines, and Processes;
- you must not use personal e-mail accounts for business purposes – do not send or forward Bank Confidential Information to these accounts; and
- it is important to ensure that only authorized Employees of Scotiabank create and send digital communications to the general public, including through social media and e-mail.

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

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 in relation to digital communications and social media apply wherever you happen to be; whether in a Scotiabank workplace or off-premises.

For specific guidelines for social media usage, please refer to Scotiabank's *Social Media Policy*.

Principle 5

Treat everyone fairly, equitably, and professionally

I. Diversity, Equity, Inclusion and Human Rights

II. Workplace Health and Safety

Principle 5

Treat everyone fairly, equitably, and professionally

This includes customers, employees, shareholders, suppliers, service providers, governments, regulators, competitors, the media and the public

Scotiabank is committed to respecting and promoting 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 and advancing an equitable and inclusive work environment that supports the productivity, personal goals, dignity and self-respect of all.

This includes commitments to:

- having a work force, at all levels of the organization, that reflects the diverse population of the communities it serves;
- providing reasonable accommodation to people who may face accessibility barriers. This includes enabling Employees to thrive and belong in the workplace, and customers who receive products or services from Scotiabank; and
- creating a safe, equitable and inclusive environment where Employees can speak up without fear of Retaliation.

I. DIVERSITY, EQUITY, INCLUSION AND HUMAN RIGHTS

Discrimination and Harassment

Scotiabank is committed to providing an inclusive, equitable, respectful and safe environment that is free from Discrimination and harassment for all as well as to complying with applicable Laws pertaining to Discrimination, human rights, and harassment. This applies to all Employees, Contingent Workers, Directors and officers of the Bank. Your actions are expected to be consistent with these principles and any related legal requirements. We also expect that the third parties dealing with Scotiabank share our commitment to respect human rights, as set out in our Supplier Code of Conduct.

Harassment, including sexual harassment, can be a form of Discrimination where there is conduct, comment(s), gesture(s), or contact related to protected ground(s):

- that is likely to cause offence or humiliation to any individual (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 Discrimination or harassment will be dealt with promptly, and treated with seriousness, sensitivity and confidentiality in accordance with applicable policies. Retaliation against anyone for having raised concerns or complaints in good faith is forbidden and anyone who has raised concerns in good faith are protected from Retaliation under this Code and under relevant policies, for example the *Global Principles on Non-Discrimination in the Workplace*, the *Global Harassment Policy* as well as local policies. If Retaliation is a concern, you can make use of the confidential Whistleblower channel.

> Diversity, equity, inclusion, and access is important to the Bank. This is why Scotiabank furthered its commitment to human rights as it became the first Canadian bank to adopt the UN Global LGBTI Standards for Business, as well as signing onto the UN Women's Empowerment Principles.

For more information on Scotiabank's global policies with respect to harassment and Discrimination, refer to the *Human Rights Policy*, *Global Principles on Non-Discrimination in the Workplace, Global Harassment Policy* and applicable local policies.

For more information on Scotiabank's human rights commitments that align to the *UN Guiding Principles on business and Human Rights*, refer to our Global Human Rights Statement.

II. WORKPLACE HEALTH AND SAFETY

Scotiabank is committed to providing 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 *Global Raise a Concern Policy* or applicable local policies; and
- treating all those you deal with respectfully and professionally, and never acting in a violent, threatening or abusive manner.

Scotiabankers who hold managerial or supervisory roles may have additional health and safety related responsibilities and should be guided by any supplementary local requirements, as applicable.

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 Voluntary Commitments and Codes of Conduct

Principle 6

Honour our commitments to the communities in which we operate

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, Guidelines, and Processes with respect to, for example, environmental credit risk, enhanced social and environmental guidelines for project finance loans, and responsible environmental management of our operational footprint. Scotiabank's *Environmental Risk Management Policy* outlines our approach to managing the Bank's direct and indirect environmental impacts. In 2019 Scotiabank announced its *Climate Commitments*, which describe the Bank's approach to addressing the risks and opportunities arising from climate change. These five commitments are detailed in an External Position Statement.

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.

You are expected to be aware of and comply with those Policies, Procedures, Guidelines, and Processes that apply to your area of responsibility.

II. CHARITABLE AND COMMUNITY ACTIVITIES

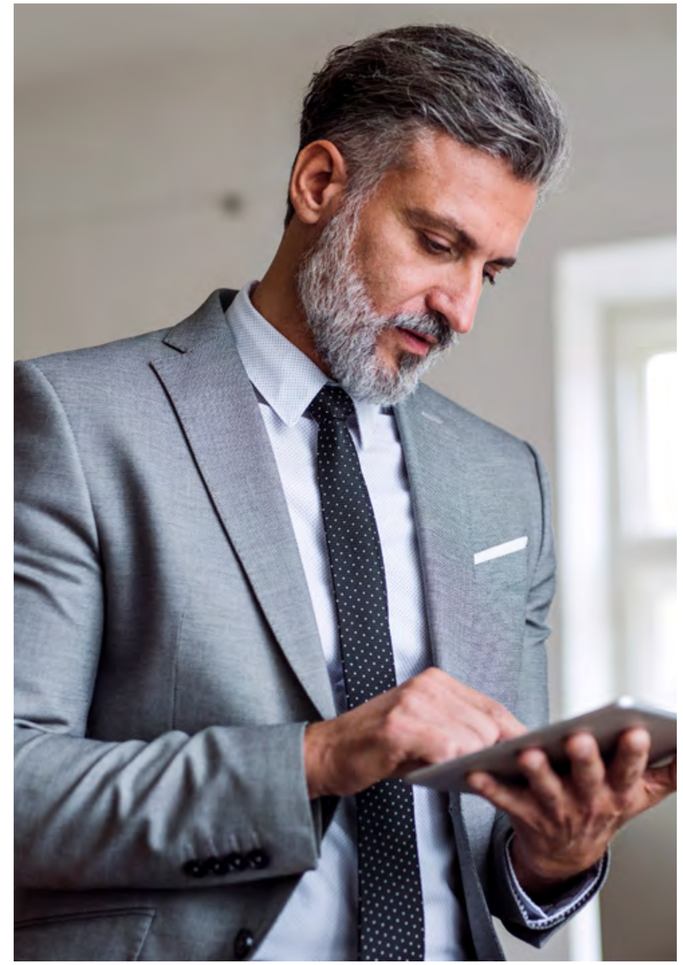
We are committed to making a positive contribution to the communities in which we operate. All donations or support given on behalf of Scotiabank should be made in accordance with the *Global Philanthropic Sponsorships and Charitable Donations Policy* and applicable Policies, Procedures, Guidelines, 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, charitable and community activities are to be limited to non-business hours.

III. POLITICAL ACTIVITIES

a. Political activities and donations in the name of Scotiabank

To avoid conflicts of interests with political or state entities or the perception of an attempt to encourage favourable treatment of the Bank or a Subsidiary, Scotiabank does not make political contributions.



Principle 6

Honour our commitments to the communities in which we operate

b. Personal political participation

Scotiabank considers participation in the political process t o 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 anyone 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.

However, the time and attention devoted to these activities should not interfere with your job performance, or present any other kind of conflict. Before running for office or accepting 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.

Any questions about your involvement in political fundraising events or activities should be directed to the Government Affairs Department.

IV. OTHER VOLUNTARY COMMITMENTS AND CODES OF CONDUCT

Some countries, Subsidiaries or specialized areas may have voluntary commitments or codes of conduct that apply to you (e.g., industry codes of conduct).

a. Commitments by Scotiabank

It is important that we honour our public commitments and adhere to voluntary undertakings to which Scotiabank has agreed to be bound. Scotiabankers are expected to be aware of and comply with those 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 a Scotiabanker comes across an instance where a 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.

Scotiabankers should acquaint themselves with these voluntary commitments or codes of conduct as they may be required to acknowledge them on an annual or other basis.

Glossary

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

Bank or Scotiabank means The Bank of Nova Scotia (BNS), including domestic and international locations, and all wholly owned or controlled Subsidiaries of BNS.

Board of Directors means the Board of Directors within BNS, Subsidiaries, or affiliates, unless specified.

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

Computer System means any technology device that accepts information (in the form of digitalized data) and manipulates it based on a program or sequence of instructions on how the data is to be processed. Examples include, but are not limited to: desktops, servers, laptops, mobile devices and tablets.

Confidential Information refers to any information that is treated as confidential by the Bank, and includes trade secrets, technology information, information pertaining to business operations and strategies, and information pertaining to customers, pricing and marketing.

Conflict of Interest arises when a person or corporation is in, or perceived to be 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.

Contingent Worker means:

- agency workers where Scotiabank has a contract with an agency who is the employer of a worker or has retained a worker who is assigned by the agency to provide services to Scotiabank; and / or
- independent contractors, where Scotiabank has entered directly into a contract with an individual (or the company owned by an individual) to provide services to Scotiabank directly.

Contingent Workers are not employed by Scotiabank and are therefore not paid via payroll by Scotiabank. Various terms may be used to address Contingent Workers throughout Scotiabank globally, including, but not limited to, third party workers, agency temps, freelancers, independent contractors, consultants, and external contractors. Our Code only applies to those Contingent Workers with access to Scotiabank networks / systems and applications as part of their job duties, globally, and any reference in our Code to "Contingent Workers" will only include those Contingent Workers with access to Scotiabank systems (platforms containing company, Employee or customer information and data) as part of their job duties.

Data Loss Prevention (DLP) is a process designed to protect confidential data and reduce the risk of it being compromised. This monitoring process helps protect both the data that Scotiabank is entrusted with as well as the Scotiabank community from the potentially serious consequences of losing confidential data, including financial penalties, customer dissatisfaction, increased regulatory scrutiny, and reputational damage.

Director means a member of the Board of Directors of a Scotiabank entity.

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 identity or expression, sexual orientation, marital status, family status, 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.

Employee(s) means any employee of Scotiabank who is paid via Scotiabank payroll including officers, Directors, full-time, part-time, temporary, and casual or contract Employees.

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

Global Raise a Concern Policy means Scotiabank's published document, "Global Raise a Concern Policy". Employees or Contingent Workers of Subsidiaries should read this and words such as "Manager" and "department head" in the context of their organizational structure and escalation processes.

Information Barriers are the Policies, Procedures, Guidelines, 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.

Glossary

Information Security & Control or "IS&C" is an organization committed to managing information security and cybersecurity effectively and efficiently. IS&C is responsible for the development and execution of the Global Cybersecurity strategy related to the identification, protection, detection, response to, and recovery from cyber-attacks, minimizing impact to the Bank.

Inside Information is Material Information that has not been generally disclosed to the public. See also "Material Information".

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."

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.

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 means an act or attempted act to disguise the source of money or Assets derived from criminal activity.

Personal Information means Information about an identifiable individual. Refers to any information that permits the identity of an Individual to be directly or indirectly inferred, including information that is "linked" or "linkable" to that Individual. This includes, but it is not limited to, name, age/date of birth, address, credit scores, net worth, and government issued identification numbers, such as Social Insurance Number.

Policies, Procedures, Guidelines and Processes refer to all applicable manuals, handbooks, job aids, forms, policies, practices, procedures, processes, guidelines, 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.

Reasonable and Occasional Personal Use is any non-business activity performed on a Bank owned asset that does not consume significant amounts of resources, does not interfere with business operations or staff productivity, does not impede monitoring controls, and does not introduce increase risk to the Bank, its Employees, customers, shareholders, or the informational Assets entrusted to the Bank.

Retaliation is any adverse action, reprisal, retribution or act of revenge taken against an Employee who has raised an issue or reported a workplace concern in good faith. Examples can include statements, conduct or actions that involve termination of employment, demotion, suspension, harassment or discrimination.

Scotiabanker(s) means Employee(s) and Contingent Worker(s) of the Bank.

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

Terrorist Financing means the collection, use or possession of money or Assets, or the provision of financial or other related services, for terrorist purposes.

Tipping is the unlawful disclosure of Inside Information about an Issuer to a person who is not authorized to have such information.

Wrongdoing is any violation or suspected intent to violate the law, this Code, a policy or procedure of the Bank, or any public commitment made by the Bank.

You means Employees, Contingent Workers, and Directors.

Guidance and advice

KEY SOURCES

If you have questions or concerns or wish to report to a more senior officer within the Bank, **use one of the options in the *Raise a Concern How-to-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	Submit a confidential, anonymous report through the Whistleblower Policy (Enterprise-wide) website at Scotiabank.EthicsPoint.com (English, French or Spanish language).
Bribery and corruption	Refer to the *Scotiabank Global Anti Bribery & Anti-Corruption Policy* or email: Conduct.Risk@scotiabank.com
Criminal activity (known or suspected)	Incidents may be reported to Corporate Security by phone during business hours at (416) 866-6666 or cs.intake@scotiabank.com After hours emergencies should be reported to the Security Operations Centre at (416) 866-5050 or CS.SOC@bns.scotiabank.com
Customer complaint resolution policies or procedures	Escalated Customer Concerns Office – 1-877-700-0043 Email: escalatedconcerns@scotiabank.com All others: Your designated Compliance Department
Conflict of interest (Bank insider and corporate client conflicts)	Compliance Control Room (Toronto) E-mail: compliance.controlroom@scotiabank.com
Conflict of interest (other)	Your designated Compliance Department or Global Compliance, Enterprise Conduct, Risk Culture & Ethics (Toronto) E-mail: Conduct.Risk@scotiabank.com
Harassment	Employee Relations, by contacting Ask HR (in Canada) or Your local Human Resources Department or if Retaliation is a concern, submit a confidential, report through the Whistleblower Policy website at Scotiabank. EthicsPoint.com.(English, French or Spanish language) or Refer to the Whistleblower Policy
Inside information, information barriers, trading restrictions and Insider Trading	Compliance Control Room (Toronto) E-mail: compliance.controlroom@scotiabank.com
Legal matters	Your designated Legal Department or Legal Department, Legal and Corporate Affairs (Toronto)
Media enquiries	Your designated Global Communications representative or Corporate and Government Affairs Executive Offices (Toronto)

Guidance and advice

KEY SOURCES

If you have questions or concerns or wish to report to a more senior officer within the Bank, **use one of the options in the *Raise a Concern How-to-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
Money laundering / terrorist financing or sanctions (known or suspected)	Your designated Anti-Money Laundering Compliance Officer or Local Sanctions Officer or AML Risk Executive Offices (Toronto)
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: staff.ombudsman@scotiabank.com
Privacy, including releasing information and breaches of privacy (customers, employees or other individuals)	The Canadian Branch Network: Please contact ask.operations@scotiabank.com or 1-844-301- 8822 All others: Use one of the options in the *Global Raise a Concern Policy* guide or contact your designated Compliance Department or Enterprise Privacy Office (Toronto) E-mail: privacy@scotiabank.com
Procurement (sourcing, contracting and purchasing) inquiries	Global Procurement Services (Toronto) Email: AskGPS@scotiabank.com
Releasing information about Scotiabank	Your Manager, supervising office or department head, as well as Corporate / Global Communications
Safeguarding Scotiabank facilities and assets	Security Operations Centre at (416) 866-5050 or CS.SOC@bns.scotiabank.com
Safeguarding electronic information (cyber-crime and data security matters, e.g. Data Loss Prevention)	Information Security & Control (IS&C) Cybersecurity Hub: http://scotiabanklive.cs.bns/community/en/its/isc E-mail: asksecurity@scotiabank.com To report an incident, contact the 24/7 Cyber Security Hotline Phone: (416) 288-3568 / 833-970-1239 (Toll Free) Email: cyber.security@scotiabank.com
Workplace issues or concerns	Contact Employee Relations, by contacting Ask HR (in Canada), your local Human Resources Department, or one of the options in the *Global Raise a Concern Policy*