Scotiabank Code of Conduct

October 2024

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 and CEO

Contents

Introduction

The *Scotiabank Code of Conduct*[1] (our "Code") describes the standards of conduct required of employees, contingent workers[2], 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, our Code should be your first point of reference. If you see something in our Code that you don't understand, or require additional guidance, ask your manager/supervisor or a more senior officer.

I. Roles and responsibilities

Our clients trust 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.

All Scotiabankers are given a copy of or link to our Code when they join the Bank, are retained or elected, and are required to receive, read and comply with our Code, and any other applicable Scotiabank policies and acknowledge their compliance within the required timeline on an annual basis. In addition, all employees are assigned an accountability goal focused on Keeping the Bank Safe and conducting all activities in line with our Code.

Executive management and the Board of Directors have additional responsibilities. The EVP and Chief Compliance Officer of Scotiabank is responsible for reporting on compliance with our 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 our Code[3] and must authorize changes[4] to our Code and any waivers[5].

---

1 This version of the Scotiabank Code of Conduct was last approved by the Board of Directors on October 29, 2024. The online version of this Code, available at www.scotiabank.com, is the most up-to-date, and supersedes prior versions.

2 Contingent worker means: (1) 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 (2) 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.

3 Our Code is formally reviewed, at a minimum, once every two years, or earlier if required.

4 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).

5 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 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.

II. Compliance with our Code

Unethical or illegal conduct puts Scotiabank, and in some cases its clients, shareholders, employees and other stakeholders, at risk. For example:

- Scotiabank and/or employees, contingent workers, directors, and officers could be subject to criminal or regulatory sanction, loss of license, lawsuits or fines; and
- Negative publicity from a breach of our Code could affect our clients' or potential clients' confidence and trust in Scotiabank, and their willingness to do business with us.

You are expected to be aware of and comply with all applicable Scotiabank policies, procedures, guidelines, standards, and processes.[6] Adherence to both the letter and the spirit of our Code and applicable policies is therefore a condition of employment at, or a contingent worker's assignment with, Scotiabank.[7] At Scotiabank, adherence to our values and ethical behaviour is encouraged, required, and reinforced through financial and non-financial incentives. Rewards and recognition motivate desirable behaviours and consequences are applied to discourage negative behaviours. By considering "how" results were achieved in addition to "what" was achieved in performance assessments, we acknowledge the importance of ethical conduct.

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.[8] Scotiabank may 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 you being subject to criminal or civil penalties.

III. Getting help or advice

If you have questions or are unsure about any of the principles or requirements of our Code, ask your manager/supervisor or another senior leader. If this is not appropriate, or if you need further guidance, consult the *Raising Concerns* section to follow, or *Key Sources of Guidance and Advice* section.

---

[6] For the purposes of this document, "policies, procedures, guidelines, standards, and processes" will be referred to as "policies".
[7] For U.S. based employees, nothing contained in our Code creates or shall be intended to create a contract of employment, express or implied.
[8] As noted in our Enterprise Risk Appetite Framework, the Bank has no appetite for breaches of our Code and consequences applied are commensurate with the severity of the breach.

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 and options available to raise a concern.

I. Obligation to report

When faced with an ethical and/or compliance issue ask yourself whether the behaviour or activity is contrary to the Bank's values, our Code, Scotiabank policies, the law, regulatory obligations, or whether it has the potential to negatively impact the Bank's reputation. You are required to immediately report these concerns, including any actual, suspected or potential breaches of our Code, such as:

- 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, systems, 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 our Code.

If a problem or concern has been referred to you, and you are unable to resolve the issue, please review the *Global Raise a Concern Policy* for further guidance on how to escalate the matter.

II. Protection from retaliation

The Bank will not tolerate any acts of retaliation against anyone that raises a concern.

Scotiabank further protects individuals by providing anonymous and confidential options to raise concerns.

III. How to report

Actual, suspected or potential breaches of our Code should be reported to your manager/supervisor, who has a responsibility to take your concern seriously, treat it with sensitivity, and respond to it in a timely manner. You also have the option to utilize one of the confidential avenues available in the *Global Raise a Concern Policy*. These avenues include reporting harassment or other workplace issues to Employee Relations by contacting AskHR (where available), or your local Human Resources department.

Alternative avenues are also available to disclose possible unethical behaviours or wrongdoing:

- The Staff Ombuds Office is available to provide confidential advice or assist in identifying an appropriate way to report your concerns. It is not a channel to report a formal complaint or ask for an investigation;
- The *Whistleblower Policy* outlines the process for reporting suspected unethical behaviour or wrongdoing (such as illegal/fraudulent activity, auditing/accounting concerns, or concerns related to retaliation), and 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; and
- The Chair of the Board is an additional avenue for escalations in situations that warrant review outside of the above (such as concerns related to the governance of the Raise a Concern program).

If you raise a concern, it will be addressed or referred to the appropriate team responsible for review and/or investigation in line with applicable policies. Staying actively engaged with and supporting the investigative process is often key to resolving concerns in a timely manner. For more detail, refer to the *Global Raise a Concern Procedures*.

Our principles

Our six Code Principles are foundational to how we live our Values (Client-centric, Integrity, Inclusion, and Accountability) and guide our behavioural expectations (Results-driven, Shaping the future, Striving for better, and Inclusive). Living up to them is an essential part of our vision to be our clients' most trusted financial partner and builds on our values-based, high performance culture.

Our six principles are:

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

Ask questions… comply… report!

Scotiabank must follow the laws that govern our business activities wherever it does business, and so must you.

You are also expected to know the internal policies that are relevant to your activities, and comply with them – both in letter and in spirit. *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/supervisor. If you need further guidance, consult the *Key Sources of Guidance and Advice* section.

Always act within the scope of your assigned authority. 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. Help make it easy to do business with us by referring clients who request advisory services to the applicable department for further guidance.

II. Conflicting requirements

In the case of any conflict between the provisions of our Code and any laws, regulatory requirements or any other policies applicable to your position, you must adhere to the more stringent requirement.

If you encounter a situation where our Code or other Scotiabank policies appear to conflict with cultural traditions, business practices or legal requirements of the country you are located in, you must consult with the Compliance Department.

PRINCIPLE 2

Avoid putting yourself or Scotiabank in a conflict of interest position

I. Personal conflicts of interest

Employees, directors, and contingent workers have an obligation to act in the best interests of Scotiabank. A conflict of interest refers to situations where a person or corporation's objectivity is undermined because they are in a position to derive personal benefit from actions or decisions made in their official capacity. This 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 a real 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 a real one.

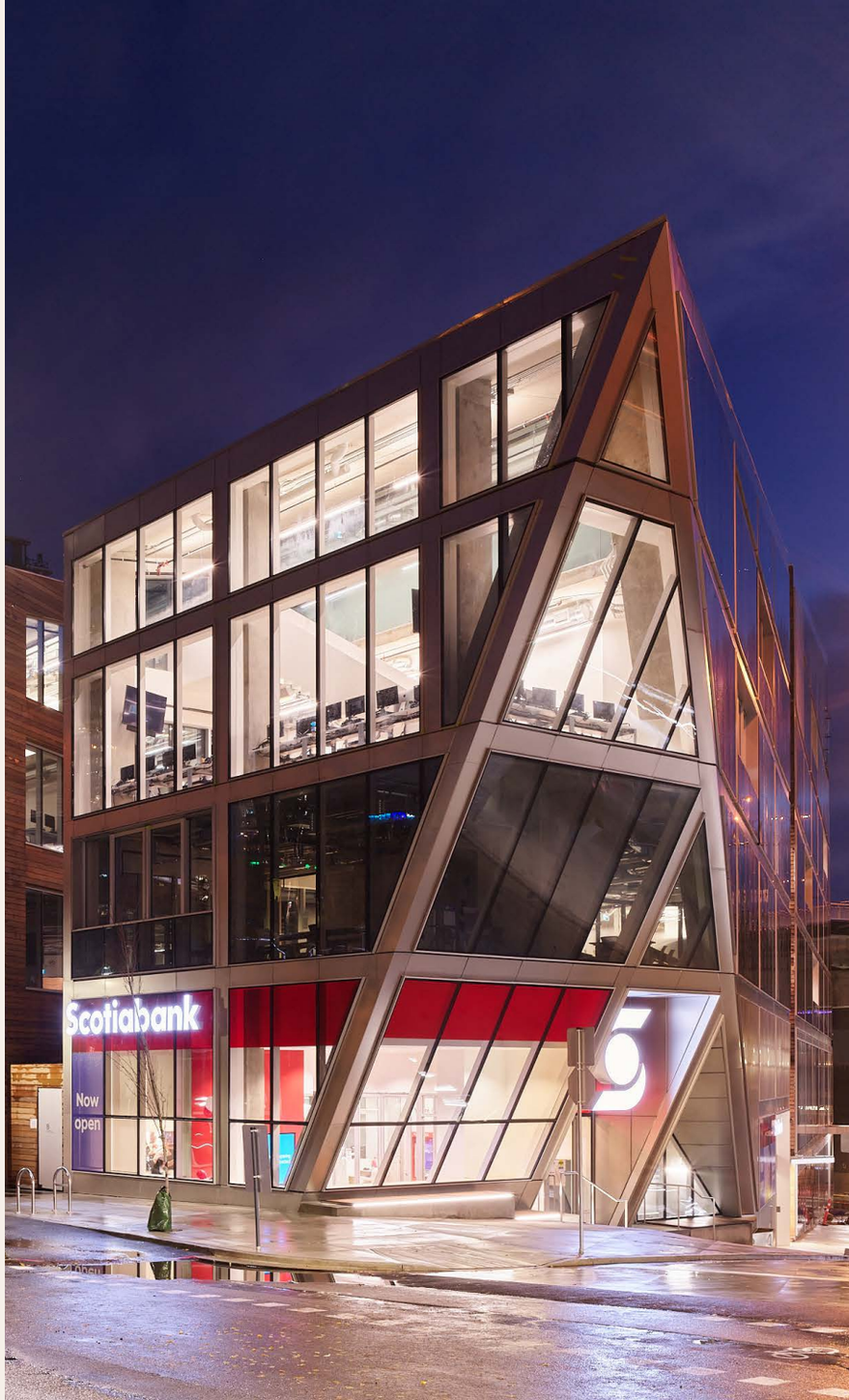
If you find yourself in a conflict of interest position or a situation where you believe that others perceive you to be in a position of conflict, you must immediately disclose this to your manager/supervisor.

Your manager/supervisor, 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 provide advice on what to do if you encounter any of these situations.

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

When Scotiabankers deal with the Bank as a client, their accounts must be established and account activities conducted in the same manner as those of any non-employee client[9] (i.e. using the same systems and facilities, such as an ABM or online/mobile banking) and without using internal systems to access their personal client profiles and accounts.



[9] Note: This is subject to any special policies or procedures that may be applicable to individuals in certain job functions, business units or subsidiaries.

The account activities of family members, friends and other close associates must also be established and conducted in the same manner as those of other clients. For example, Scotiabankers must not set up accounts for themselves, or on behalf of these individuals, access their profiles or transact any business without the review and agreement of their manager/supervisor and with appropriate authorization from the client.

Under no circumstances may you authorize or renew a loan, or lending or margin limit increase to yourself, a family member, a friend or other close associate. You may not waive fees, reverse charges or confer any benefit or non-standard pricing or access client system 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/supervisor.

b. Close personal relationships in the workplace[10]

Real or perceived conflicts of interest also can arise when Scotiabankers work with someone they share a close personal relationship with (such as family relationships, romantic relationships and/or financial relationships[11]) and can also raise serious concerns about favouritism and, in certain cases, the validity of consent.

In accordance with the *Close Personal Relationships in the Workplace Policy (Global)*, Scotiabankers must immediately disclose real or perceived conflicts of interest related to close personal relationships in the workplace to their manager/supervisor or through one of the options in the *Global Raise a Concern Policy*.

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 client's needs, engaging a supplier or service provider, or hiring an individual on a strictly business basis.

You have a responsibility to escalate any external attempts (e.g., by foreign or domestic actors) to influence your or any Bank employee's objectivity through one of the options in the *Global Raise a Concern Policy*.

d. Outside business activities, financial interests or employment

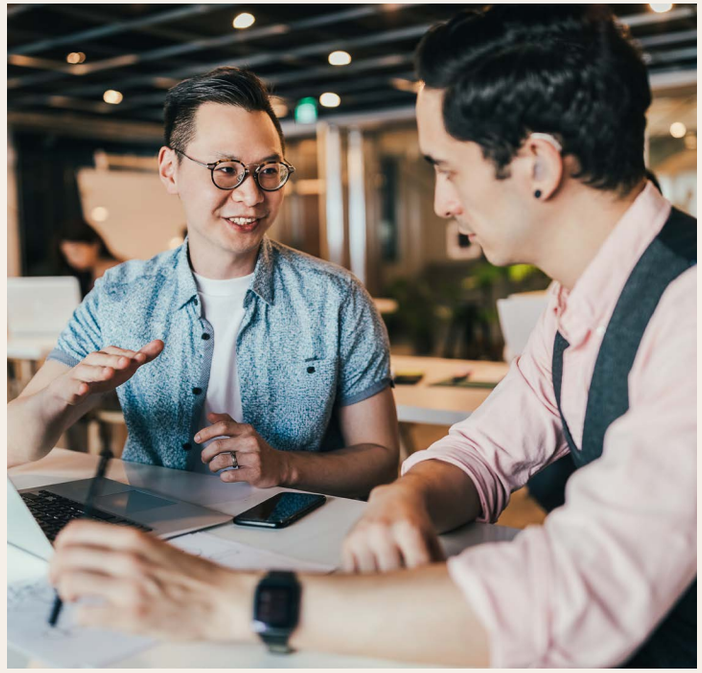
For employees, having other work (paid or unpaid) outside of your employment with Scotiabank is permitted if there is no conflict of interest and if the satisfactory performance of your job functions with Scotiabank is not prejudiced or negatively impacted in any way.

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 or Scotiabank equipment or facilities;

[10] Please refer to Footnote 9.

[11] For example, having obligations as a power of attorney, an executor, a trading authority, a business partner in outside business activities etc.



- Employees 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, or position;
- Employees cannot solicit Bank clients to take part in their outside business activity. For example, if an employee were to work as a real estate agent while also working for Scotiabank as a financial advisor in a branch would give rise to a real or perceived conflict of interest, as the employee can personally benefit from selling real estate by soliciting Bank clients while also arranging the financing;
- Neither employees nor members of their household should have a financial interest in, or with, a client, 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;[12] and
- Employees should seek approval from their manager/supervisor (or department head, where appropriate) prior to taking on an outside business interest. If your manager/supervisor 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.

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/supervisor and/or your Business Line Compliance Department to be sure the proposed outside business activities do not create a conflict.

e. Misuse of confidential information

You are regularly entrusted with confidential information that may not be publicly known about Scotiabank, its clients, 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. Except as provided in Principle 3, s. VI, Audits, Investigations, and Regulatory Reporting, it is 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.

f. Directorships

Employees or officers may not accept a corporate directorship until obtaining approval/concurrence from their manager/supervisor and, where applicable, the Compliance Department.[13] The Compliance Department will seek any other necessary approvals. New employees must immediately report any directorships and seek approval where necessary.

For further information on your obligations, refer to the Scotiabank Corporate Directorships Policy.

g. Wills, other trusteeships and similar appointments

We expect employees to decline any client who suggests leaving a gift in their will, as this could create a perception that you manipulated or took advantage of the client.

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

[12] This policy does not apply to holdings in the publicly traded securities of suppliers or clients, as 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*.
[13] 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.

If employees are named as a beneficiary, executor, administrator or trustee of a client's will or other trust document, other than as a family member, report the gift or appointment and the nature of the relationship to your manager/supervisor, who will consult the Compliance Department. 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 unfair 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.

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.[14]

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 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 clients. For example:

- Scotiabank's interests could conflict with its obligations to a client;
- Scotiabank's obligations to one client could conflict with its obligations to another; or
- Scotiabank's relationships with one third party supplier could conflict with its obligations to another 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. For example, if Scotiabank were asked to lead financing for more than one client's bid on the same asset, a perception may arise that one client may be given preferential treatment over another.

Those who become aware of a potential conflict must observe policies regarding confidentiality and conflicts of interest and advise their manager/supervisor or Compliance contact as set out in the *Key Sources of Guidance Advice* section 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 employees are also not permitted to use Bank resources or the Bank's name to help organize, promote or host political fundraisers.

[14] 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

Our success depends on your honesty and integrity. Always remember that your conduct has a direct effect on how clients think about Scotiabank and how it reflects on you.

I. Illegal or fraudulent activities

a. Misappropriation

Stealing funds or information, attempting to defraud a client or Scotiabank, or knowingly helping others to do so is a serious violation of our Code. 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 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 have a responsibility to protect against data loss, misuse, and/or mismanagement. Only access and use records, computer files and programs (including personnel files, financial statements, online client and employee profiles and other client or employee information and/or data) for their intended, Scotiabank-approved purposes.

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 use.

Improperly accessing records

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

Any access to Bank records without authorization is a privacy breach and a breach of our Code.

c. Creating false records

Forgery or creating false records (including false signatures) is a crime, a betrayal of client trust and a serious violation of our Code – even if there is no intention to defraud. This includes creating Know Your Client records that you know are false or misleading.

It is also fraudulent to knowingly make or allow false or misleading entries to be made to any Scotiabank account, record, model, system or document (this includes, but is not limited to, inflating sales numbers to receive higher commissions, falsifying sales that did not occur or colluding with clients 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 in accordance with the *Global Raise a Concern Policy*.

d. Bribes, payoffs and other corrupt practices

Scotiabank prohibits any form of bribery and corruption. This means:

- Employees and third parties working with Scotiabank must follow the *Scotiabank Global Anti-Bribery & Anti-Corruption Policy* and all applicable anti-bribery laws;
- Employees must not (directly or through an intermediary) offer, give, solicit, accept or authorize, **anything of value** including facilitation payments to or from public officials, Politically Exposed Persons ("PEP")[15], business partners, clients, or others in exchange for improper advantage or consideration. Employees must be aware that payments made indirectly through any third-party intermediary are considered as payments made by Scotiabank and are subject to the same regulations;
- Only engaging suppliers/vendors/service providers after conducting appropriate due diligence and on the basis of their credentials, skills and qualifications; and
- Employees must immediately report actual or suspected incidents of bribery or corruption following the process outlined in the *Global Raise a Concern Policy*.

For additional guidance, refer to the *Scotiabank Global Anti-Bribery & Anti-Corruption Policy* or contact the Compliance Department.

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 of this information may be 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 or Material Non-Public Information (MNPI) and you may not act on this information for the benefit of yourself, a close friend, or a relative 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 conduct your securities trading only through brokerage accounts monitored by Scotiabank as well as impose other rules.

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

There are very strict laws forbidding both insider trading and tipping, and violations carry severe penalties.

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

f. Other trading restrictions

You may not engage in trading or other activities intended to improperly influence or manipulate markets and are prohibited 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/supervisor, 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 a charge or conviction.

h. Anti-competitive practices

To promote fair and open competition, 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 clients 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); and
- Provide or receive competitively sensitive information.

Do not engage in other anti-competitive activities, including tied selling, abuse of dominance, false/misleading advertising, and other deceptive marketing practices. Be cautious entering into wage-fixing or no-poach agreements as these may be prohibited in some jurisdictions.

You may participate in industry associations or events (including Bank-approved related benchmarking exercises), but these meetings and interactions 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 client

Knowing your clients helps to better serve their needs, meet regulatory requirements, avoid facilitating activity that is outside of our risk appetite, 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 client transactions must be authorized and handled in an approved manner and must adhere to applicable standards for knowing your client. Do not undertake, participate in, or facilitate any client 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 clients are serious international problems that lead to harmful legal, economic, and social consequences. Familiarize yourself with the policies related to anti-money laundering, anti-terrorist financing, anti-bribery and anti-corruption, and compliance with sanctions that are applicable to your role.

Scotiabankers must promptly report any unusual account activity to their manager/supervisor 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 suspicious transaction or warning a client that a report has been or will be made about them is a breach of our Code and may be viewed as a criminal offence.

III. Ethical business practices

a. Offering and accepting gifts and entertainment

Offering and/or accepting gifts and entertainment is a common way business partners show their appreciation and respect for each other. However, do not offer and/or accept gifts and entertainment if they:

- Create the appearance of improper influence or a quid pro quo arrangement;
- May be perceived as offer or acceptance of a bribe and/or kickback;
- May appear to impair the recipient's objectivity and independence;
- Violate legal and regulatory obligations; or
- Have the potential to harm Scotiabank's reputation.

Key principles that govern the giving and accepting of gifts and entertainment:

- Gifts and entertainment must be modest[16] and infrequent, and must not be illegal or inappropriate (e.g., adult entertainment);
- Gifts and entertainment to or from public officials or PEPs (of any value) should be avoided, and in some jurisdictions they are prohibited;

[16] 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.

- Never give, receive, offer, or authorize gifts and entertainment during or immediately before or after entering into negotiation or while awaiting or awarding/ renewing a contract;
- Obtain requisite prior approvals/approvals, when appropriate, and respect the thresholds and limits defined within the *Scotiabank Global Gifts and Entertainment Policy* and applicable Gifts and Entertainment Operating Procedures;
- Ensure it is not a gift of cash or a cash equivalent, bond or negotiable security, or personal loan; and
- Ensure all gifts and entertainment expenses are transparently recorded.

Please review the *Scotiabank Global Gifts and Entertainment Policy* and direct any questions to ge@scotiabank.com.

b. Charitable donations or community sponsorships

The Bank remains firmly committed to creating a more inclusive and resilient society for everyone, and for every future. However, it is important to note that charitable organizations can be used as fronts or conduits for improper payments, including those made for the purpose of obtaining an unfair business advantage. Offering charitable donations or community sponsorships 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;
- Appear to impair the recipient's objectivity and independence;
- Violate legal and regulatory obligations; and
- Harm Scotiabank's reputation.

For additional guidance, please refer to the Global Donations and Community Sponsorships Policy and the Scotiabank Global Anti-Bribery & Anti-Corruption Policy.

c. Dealing ethically with our clients, employees and others

We do not compromise our ethics for the sake of profit, or for meeting sales targets or goals.

Steering a client to an inappropriate or unnecessary product harms the client, 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 clients or the public must consult their manager/supervisor 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 close personal relationships, or family, political, governmental or other affiliations. 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.

Coercive tied selling

Never pressure clients to buy a product or service that they do not want as a condition for obtaining another product or service from Scotiabank (coercive tied selling).

This should not be confused with other practices, such as giving preferential pricing to clients 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.

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 clients or other business relationships.

For example, you must not use your connection with Scotiabank:

- So that you, or anyone you have a close personal relationship with, can borrow from or become indebted to clients; or
- To gain preferred rates or access to goods and services[17], whether for yourself or anyone you have a close personal relationship with, unless the benefit is conferred as part of a Scotiabank-approved plan.

d. Respect intellectual property rights

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

Use only applications and hardware provided through Scotiabank Technology and Operations. 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 our Code, and the guidance on respecting intellectual property laws set out within.

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 clients' data. The collection and creation of data should be done to deliver the best banking experience to our clients and with their interests in mind. In order to do that, and to maintain our clients' 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.

For more information, refer to Scotiabank's Data Ethics Commitment.

[17] 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.

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* and should engage only those who are competent and reputable, and who have business conduct standards comparable to our own. Service providers, suppliers 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.

The *Global Third Party Risk Management Policy* is applicable to and must be followed for all third party arrangements with external third parties and intragroup entities.

Do not disclose any confidential or proprietary information of a third party supplier to any other third party without obtaining their prior written consent and advice from the Legal Department. Additionally, it is essential that you protect client and employee data, and do not disclose it to any third party supplier without obtaining written consent and advice from Customer Insights, Data & Analytics (CID&A) and Information Security and Control (IS&C).

V. Communications and representations

Trust is the basis of our relationships with our clients, fellow employees, shareholders and the communities in which we operate. You must not knowingly mislead clients, 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). Advertisements must be accurate, clear and not misleading. This includes representations by third parties made on behalf of Scotiabank (such as influencers and 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 Investor Relations or Global Communications.

c. Making public statements and media contact

Scotiabank is subject to laws and regulations that prohibit communicating false or misleading information to a client or to the public. All media inquiries must be referred to Global Communications. Only spokespeople authorized by Global Communications can speak to the media on behalf of the Bank. 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 clients, employees and others.

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 they receive required approvals for any public speaking events they are asked to participate in. Even if you are presenting in your own personal capacity and you've made that clear, please remember that by the nature of your title, the public may still interpret your views as Bank views. For guidance, please see the *Media Relations Policy & Guidelines* and *Social Media Policy*.

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/supervisor 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 good judgement when offering your personal opinions in a public forum (such as social media, internet blogs, or newsgroups), taking care not to disparage Scotiabank, its products and services, or competitors, while always protecting confidential information about Scotiabank, clients, employees or others.[18]

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. Audits, investigations, and regulatory reporting

Always cooperate fully with any investigations by management or Compliance, Legal, Internal Audit, Corporate Security, Information Security & Control, Fraud Management, or Human Resources. 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 and Information Management Policy*.

Scotiabankers may choose to report conduct that they believe is unlawful to a regulator or member of law enforcement, and Scotiabankers who choose to do so are not required to inform the Bank of this action. Additionally, Scotiabank has a responsibility to report certain incidents to regulators and law enforcement as required by law.

[18] For U.S. based employees, you should refrain from making statements about Scotiabank or its employees, officers, and directors that are knowingly false or made with reckless disregard for the truth.

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 clients, 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

You are expected to be aware of, and follow, the policies 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 *Privacy Incident and Breach Management Procedures*. Those policies explain how to report, respond to and remediate a breach of privacy or confidentiality.

Confidential information refers to any information where loss could lead to unacceptable risk, and includes trade secrets/technology information, and information pertaining to business operations/strategies, and/or clients, pricing and marketing. All information about current or prospective clients, employees or others should be presumed to be confidential unless the contrary is clear.

Never access personal information (including your own file) or confidential business information about Scotiabank, a client, or an employee without a legitimate business reason and appropriate authorization. For example, do not view client profiles or account information of family members, friends, acquaintances, or employees without a valid business reason to do so. Accessing someone's personal information without valid authorization or permission is a breach of the law and our Code.

Never access, collect, disclose or use confidential information or proprietary information obtained from third parties, other organizations or former employers without proper authorization. Taking confidential information as you leave the Bank with the intent to use it for future business activities may also lead to civil or criminal action against you, even if you are no longer a Scotiabank employee.

b. Appropriate handling of personal and confidential information

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

Appropriate handling of personal and confidential information includes the following

- Follow policies and supporting documentation for storing, handling, and controlling access to personal and confidential information.
- Use the Scotiabank Secure Email Service procedures where personal and confidential information must be sent outside Scotiabank. See the *Key Sources of Guidance and Advice* section for more information.
- Do not carelessly display personal or confidential information to others.
- Do not disclose personal or confidential information to anyone outside Scotiabank (including family or household members or close associates) or to others who do not require the information for their work *(except as provided in Principle 3, s. VI. Audits, Investigations, and Regulatory Reporting)*.
- Destroy or dispose of information according to security requirements and policies for document retention and destruction.

You must ensure that any new Scotiabank initiative or service and any new use of personal and confidential information that you are involved with has undergone a Privacy Impact Assessment and/or 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/supervisor or through one of the options described in the *Key Sources of Guidance and Advice* section or in the *Global Raise a Concern Policy* so that steps can be taken to prevent, minimize or mitigate any negative impact on clients, employees, other stakeholders, or Scotiabank.

c. Disclosures of personal and confidential information

Third parties sometimes request information about clients (including family and friends) or employees. Subject to legal exceptions, you must obtain consent before releasing a client's personal or confidential business information to anyone else. This includes releasing information about whether or not an individual, business or government department is actually a client. Legal Department assistance may be required to verify requests for information without consent.

II. Accuracy and integrity of transactions and records

The expectations of our clients, 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 to ensure that transactions:

- Have a legitimate business purpose (e.g., do not mislead regarding earnings, revenue or balance sheet values, or any action resulting in an unethical or illegal outcome);
- Are properly authorized and adequately supported by back-up documentation; and
- Are promptly and accurately recorded in the right accounts.

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.

III. Security

a. Keep Scotiabank and client assets safe

Be alert to the potential for harm, loss, corruption, misuse, unauthorized access or theft of Scotiabank or client assets, **no matter where you are working**. These include:

- Funds and negotiable instruments;
- Technological devices and resources (e.g., computer systems and networks, telecommunication systems, communication channels, and the Internet);
- Physical property, premises, supplies and equipment;
- Intellectual property, including Bank-developed software; and
- Personal and confidential information, however stored or maintained, including information held on electronic storage devices.

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

b. Appropriate use of information technology and services

Scotiabank monitors its information technology systems, services, and facilities to prevent and detect the harm, loss, corruption, misuse, unauthorized access or theft of Scotiabank or client assets.

Information technology and services are provided to you to enable you to do your job. Examples include Bank-issued devices such as laptop, PC, phone, and tablets running approved software installed through information technology. Any other use, except for reasonable and occasional personal use, is not allowed.

Additional responsibilities include the following:

- Ensure business communications are only conducted using approved communication channels on Bank-issued devices, in line with the Global Voice and Electronic Communications Policy. The use of unauthorized communications channels for business communications is considered a breach of our Code;
- Advise Scotiabank (as soon as is reasonably practical) if your Bank-issued device is lost or stolen (e.g., laptop, phone);
- Ensure proper operating system and application updates/patches are installed as soon as they are available;
- Do not bypass or interfere with security controls or the system configuration of any Bank-issued devices (e.g., sharing access credentials and passwords, installing your own software, “jailbreaking” mobile devices, “rooting” computer systems); and
- Only access, conduct business using, or store Bank information in public Internet services approved by the Bank’s designated governance forums.

IV. Digital communications, use and representation

Inappropriate Internet usage outside the workplace could subject you, Scotiabank, its clients, or other stakeholders to legal, reputational, privacy, data, 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. For further information on inappropriate internet use outside of the workplace, please refer to the *Expressing Your Personal Views* section of this Code.

Employees are permitted to only use approved communication channels on Bank-issued devices to communicate over the Bank’s electronic networks, to discuss Bank related matters, or to access the Internet for business-related use. Use of unapproved devices, services, applications, or channels of communication to conduct business is strictly prohibited. It is important to ensure that only authorized employees of Scotiabank create and send digital communications to the public.

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. Be careful to protect information and avoid unintended disclosure (e.g., posting pictures that contain Scotiabank information, taking a photograph with a whiteboard in the background). 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 the *Social Media Policy*.

You are required to comply with all applicable policies with respect to the sending of emails and other digital communications. For specific guidance, please refer to Scotiabank *Canada’s Anti-Spam Legislation (CASL) Policy*.

PRINCIPLE 5

Treat everyone fairly, equitably, and professionally

This includes clients, 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, contingent workers, clients, shareholders, suppliers, service providers, governments, regulators, 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 clients who receive products or services from Scotiabank;
- Winning as one team by building and strengthening a culture where all Scotiabankers can thrive; and
- Creating a psychologically safe, equitable and inclusive environment where employees can speak up without fear of retaliation.

Diversity, equity, inclusion, and accessibility 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.

I. Diversity, equity, inclusion and human rights

Discrimination and harassment

Scotiabank is committed to providing an inclusive, equitable, accessible, 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, accessibility, 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*.

Discrimination means any action or a decision, without lawful justification, whether intentional or not, which has the effect of denying benefits to, or otherwise disadvantaging, an individual unfairly in the course of employment on the basis of the protected grounds (race, national or ethnic origin, colour, religion, age, sex, sexual orientation, gender identity or expression, marital status, family status, disability, genetic characteristics and a conviction for which a pardon has been granted or a record suspended, or any other grounds that apply to affiliates, subsidiaries or to Scotiabank's operations globally).

Harassment, including sexual harassment, can be a form of discrimination where there is conduct, comment(s), gesture(s), or contact related to legally 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 sensitivity and confidentiality.

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

Scotiabank's Environmental, Social, and Governance commitment is driven by developing, implementing and investing in initiatives across our ESG pillars in order to maximize our positive impact. We earn the trust of our clients, shareholders, and each other through being transparent and honouring our commitments.

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 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. Our *Climate Commitments* outline the Bank's approach to addressing the risks and opportunities arising from climate change.

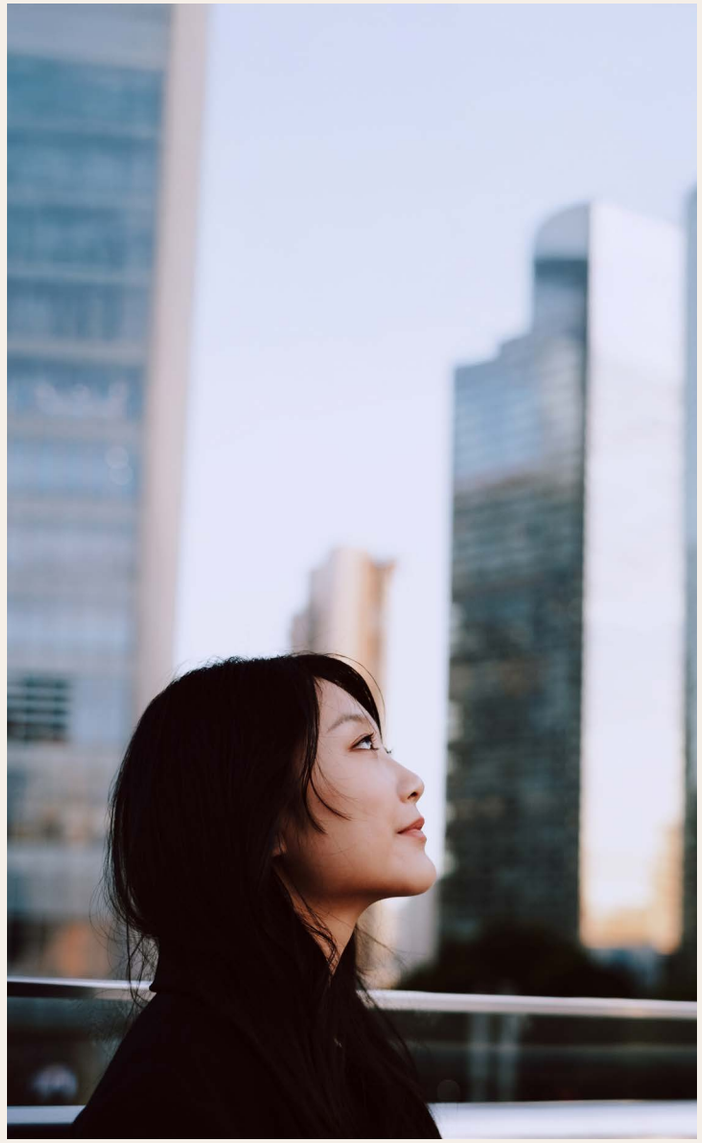
II. Charitable and community activities

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 Donations and Community Sponsorships Policy* and applicable policies.

In special cases, your manager/supervisor 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.

Charitable donations

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



III. Political activities

a. Political activities and donations in the name of Scotiabank

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.

b. Personal political participation

Scotiabank considers participation in the political process to be an important contribution to the community and a personal decision that is subject to 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/supervisor 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

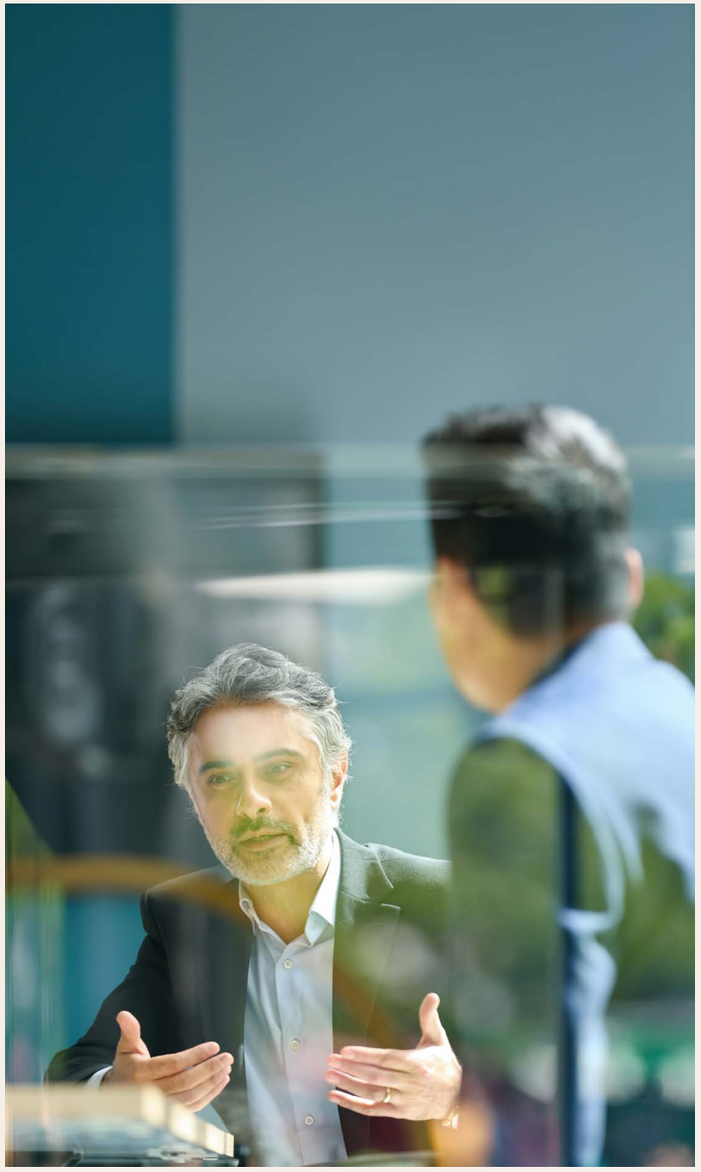
Many professions and professional bodies have codes of conduct or ethics to which they expect their members to adhere. If a Scotiabanker comes across an instance where a profession's code of conduct conflicts with our Code, inform your manager/supervisor and the Compliance Department immediately. In 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.

Key sources of guidance and advice

As appropriate, speaking with your manager/supervisor or another senior leader within your business unit is the first step in escalating your concern (please see the options in the Global Raise a Concern Policy for more information). If this is not feasible, or if you wish to pursue a different avenue for escalation or 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 report through the Whistleblower website at Scotiabank.EthicsPoint.com (English, French or Spanish language and option to remain anonymous).
Bribery and corruption	Refer to your designated Compliance Department or the Scotiabank Global Anti-Bribery & Anti-Corruption Policy or email: ABAC@scotiabank.com
Criminal activity (known or suspected)	Incidents may be reported to Corporate Security and will be handled during regular business hours (Monday to Friday 9-5 EST) at 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	Escalated Customer Concerns Office: 1-877-700-0043 Email: escalatedconcerns@scotiabank.com All others: Your designated Compliance Department
Concerns relating to senior executives or the governance of the Raise a Concern program	Concerns may be raised to the Board of Directors by emailing the Chair of the Board at chair.board@scotiabank.com in situations that warrant review outside of the regular channels.
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



Issue	Additional sources of guidance and advice
Conflict of interest	Your designated Compliance Department or Global Compliance, Enterprise Conduct, Risk Culture & Ethics (Toronto) E-mail: Conduct.Risk@scotiabank.com
Workplace concerns (treatment/harassment, etc.)	Employee Relations, by contacting Ask HR (in Canada) or Your local Human Resources Department or Submit a confidential report through the Whistleblower 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
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)
Privacy, including releasing information and breaches of privacy (clients, 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 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
Safeguarding Scotiabank facilities and assets	Security Operations Centre (416) 866-5050 or CS.SOC@bns.scotiabank.com
Safeguarding electronic information (cyber-crime and data security matters, e.g., data loss prevention)	E-mail: asksecurity@scotiabank.com To report an incident, contact the 24/7 Cyber Security Hotline Phone: (416) 288-3568 / 1-833-970-1239 (Toll Free) Email: cyber.security@scotiabank.com