

Guidelines for Business Conduct

Doing the right thing,
and acting with integrity



* Trademark of The Bank of Nova Scotia



Guidelines for Business Conduct

A Message from our CEO

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

Our reputation is something we must never take for granted. We must all strive to protect and strengthen it, if we are to achieve our goal of being the best Canadian-based international financial services company.

Doing the right thing, and acting with integrity, is essential to maintaining our good name – even when it is difficult, or seems to conflict with other priorities. Meeting sales goals or profitability targets is important, but absolutely nothing is more important than staying true to our values.

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

Please read the Guidelines carefully, think about what they mean to your own job and workplace situation, and use good judgment to apply the principles every day in your actions at work. It's not possible for the Guidelines to cover every situation, so if you aren't sure about the right thing to do, consult your Manager or a more senior officer. Consult the *Pathways to Resolution* guide – or any of the other options described in the Guidelines – to let management know about any questions or issues you encounter. Complying with the Guidelines is a condition of your employment and, every year, you will be asked to affirm that you have read the Guidelines and followed them.

By living up to the principles set out in these Guidelines, doing business with integrity and working together to sustain our core values, we can entrust future generations of Scotiabankers with the gift of the enviable reputation we have inherited.

Sincerely,

A handwritten signature in black ink that reads "Rick Waugh". The signature is written in a cursive, slightly slanted style.

Richard E. Waugh
Chief Executive Officer

Table of Contents

Introduction	4
Your Responsibilities	4
Management Responsibilities	4
Board and Executive Management Responsibilities	5
Consequences of Failing to Comply with the Guidelines	5
Supplemental Guidelines	5
Our Guiding Principles	7
Principle 1	8
Follow the Law Wherever Scotiabank Does Business	
Your Responsibilities	8
Conflicting Requirements	8
Principle 2	9
Avoid Putting Yourself or Scotiabank in a Conflict of Interest	
Personal Conflicts of Interest	9
Corporate Conflicts of Interest	13
Principle 3	14
Conduct Yourself Honestly and with Integrity	
Illegal or Fraudulent Activities	14
Improper Transaction Prevention	16
Ethical Business Practices	17
Engaging Third Parties	19
Communications and Representations	19
Cooperate With Audits and Investigations	20
Principle 4	21
Respect Confidentiality, and Protect the Integrity and Security of Assets, Communications, Information and Transactions	
Privacy and Confidentiality	21
Accuracy and Integrity of Transactions and Records	22
Security	22
Principle 5	25
Treat Everyone Fairly, Equitably and Professionally, Whether They are Customers, Suppliers or Service Providers, Employees, or Others Who Deal with Us	
Diversity, Equity and Human Rights	25
Workplace Health and Safety	25
Principle 6	27
Honour our Commitments to the Communities in which We Operate	
Environmental Protection	27

Charitable and Community Activities	27
Political Activities	27
Other Codes of Conduct and Voluntary Commitments	28
Getting Help or Reporting Problems and Irregularities	29
Obligation to Report	29
Protection from Retaliation	29
How to Report	29
Glossary	31
Key Sources of Guidance and Advice	

Introduction

The *Scotiabank Guidelines for Business Conduct** (the “Guidelines”) describe the standards of conduct required of directors, officers and [employees](#) of The Bank of Nova Scotia and its global [subsidiaries](#) (“[Scotiabank](#)”).

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

Consult the [glossary](#) at the end of this document for definitions of some of the key terms used in these Guidelines.

I. Your Responsibilities

Read... Ask Questions... Comply... Report!

New directors, officers and employees are given a copy of the Guidelines when they are elected or hired and must acknowledge that they have received and read them.

As a director, officer or employee of Scotiabank, you are responsible for ensuring that you:

- > read the Guidelines and, each year, reaffirm that you have followed them;
- > ask questions if you are unclear about your responsibilities or the appropriateness of a particular action or behaviour;
- > comply with the Guidelines, and any other Scotiabank policies that apply to your job, at all times; and
- > report any actual or potential breach of the Guidelines as soon as you become aware of it (see [Getting Help or Reporting Problems and Irregularities](#)).

II. Management Responsibilities

Be aware... Communicate... Supervise... Respond... Escalate!

If you are a Manager, you must also:

- > be aware of the [laws](#), regulatory requirements and internal [policies, procedures, and processes](#) pertinent to your area of responsibility;
- > make sure that these requirements are communicated to your employees;
- > manage and supervise your employees with the objective of ensuring that the law, the Guidelines and other policies, procedures and processes are followed;

* This version of the Guidelines for Business Conduct was approved by the Board of Directors on October 30, 2012. The online version of the Guidelines, available at www.scotiabank.com, is the most up-to-date, and supersedes printed versions.

- > respond to questions from the employees who report to you (with assistance, if required, from a more senior officer or a contact point identified in the *Key Sources of Guidance and Advice* addendum); and
- > ensure that any actual or potential breach of the Guidelines that is reported to you is dealt with or escalated in accordance with applicable policies, procedures, and processes.

III. Board and Executive Management Responsibilities

The Chief Executive Officer of [the Bank](#) bears overall responsibility for ensuring that the Guidelines are followed throughout the organization, and reports on compliance every year to the [Board of Directors](#) or a Committee of the Board. The Board of Directors is responsible for reviewing and approving the content of the Guidelines and must authorize changes[†] and certain kinds of waivers.[‡]

IV. Consequences of Failing to Comply with the Guidelines

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

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

Adherence to the Guidelines is therefore a condition of employment at Scotiabank. Any breach will be treated as a serious matter, and may result in discipline up to and including termination. Scotiabank may be required to report certain types of breaches to law enforcement or regulatory authorities. A breach may result in you being subject to criminal or civil penalties.

V. Supplemental Guidelines

You are expected to be aware of and comply with the following supplements to the Guidelines for Business Conduct:

- > *Internet and Electronic Mail Code of Conduct*; and
- > *Whistleblower Policy and Procedures* (“*Whistleblower Policy*”).

[†] Notwithstanding the Board of Directors' authority over changes and waivers of the Guidelines, Global Compliance E.O. 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).

[‡] In certain limited situations, the Bank may waive application of a provision of the Guidelines to a director, officer or employee. The Board of Directors or a Committee of the Board of Directors must approve any waivers involving a director or executive officer of the Bank, 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 the Bank's Legal, Compliance and Human Resource Departments. Waivers will be granted rarely, if ever.

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

Our Guiding Principles

Scotiabank's six Guiding Principles are the building blocks on which the Guidelines rest. Living up to them is an essential part of our meeting our corporate goals and safeguarding Scotiabank's reputation for integrity and ethical business practices.

The six principles are:

1. Follow the law wherever Scotiabank does business.
2. Avoid putting yourself or Scotiabank in a conflict of interest.
3. Conduct yourself honestly and with integrity.
4. Respect confidentiality, and protect the integrity and security of assets, communications, information and transactions.
5. Treat everyone fairly, equitably and professionally, whether they are customers, suppliers or service providers, employees, or others who deal with us.
6. Honour our commitments to the communities in which we operate.

REMEMBER:

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

FOLLOW THE LAW

Wherever Scotiabank Does Business

I. Your Responsibilities

Ask Questions... Comply... Report!

The laws of each of the countries in which we operate regulate many aspects of our activities. Scotiabank must follow the law wherever it does business, and so must you. You are also required to comply with Scotiabank's internal policies, procedures and processes. If you are unclear about legal or other requirements, consult your Manager. If necessary, he or she can seek the advice of the [Legal Department](#) or [Compliance Department](#).

Sometimes policies and procedures may seem cumbersome, but remember that they have been developed with legal requirements in mind. Be careful to always act within the scope of your assigned authority. Skipping a step, even one that seems redundant, could put Scotiabank, you, your fellow employees, customers, shareholders or others at significant risk.

Immediately report any actual, suspected or potential violations of the law through one of the options described in the [Pathways to Resolution](#) guide (or, where appropriate, under the *Whistleblower Policy*), or using the other avenues described in [Getting Help and Reporting Problems and Irregularities](#).

II. Conflicting Requirements

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

Advice That Can Put Scotiabank at Risk:

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

This is because 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.

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

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

Avoid Putting Yourself or Scotiabank in a Conflict of Interest

I. Personal Conflicts of Interest

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

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

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

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

Your Manager, who may consult a more senior Manager or the Compliance Department if necessary, will decide if a conflict exists or if the appearance of a conflict would be damaging to Scotiabank's reputation.

Some common conflicts that you may encounter, and the guidelines that you should follow if you do, are outlined below.

a. Transactions that Involve Yourself, Family Members or Close Associates

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

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

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

b. Objectivity

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

c. Outside Business Activities, Financial Interests or Employment

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

In addition, the following rules apply:

- > You should not engage in a business that competes with Scotiabank, or in any activity likely to compromise Scotiabank's position or reputation.
- > You should not conduct outside business on Scotiabank time, or use Scotiabank equipment or facilities to conduct an outside business interest. This includes soliciting other employees to participate.
- > You owe a duty to Scotiabank to advance its legitimate interests when the opportunity to do so arises. You may not take for yourself a business opportunity that is discovered in the course of your Scotiabank employment, or through the use of Scotiabank property, information or your position.

[§] Note: This is subject to any special policies or procedures that may be applicable to employees in certain job functions, departments or subsidiaries.

- > Neither you nor members of your household should have a financial interest in, or with, a customer, supplier or service provider of Scotiabank, or any other entity having a close business relationship with Scotiabank, if this would put you in a conflict of interest.**
- > Before taking on or continuing an outside business interest, making or holding a financial interest in a Scotiabank customer, supplier or service provider, or other entity having a close business relationship with Scotiabank, or committing to a job outside Scotiabank working hours, discuss this with your Manager to be sure these activities do not create a conflict. (Employees of securities or other subsidiaries may be subject to special rules with respect to outside employment, interests or activities and, therefore, may require pre-approval from their Compliance Department).

d. **Misuse of Confidential Information**

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

e. **Directorships**

Obtaining Approval: As an officer or employee, you may not accept a corporate directorship unless you have obtained approval from your Manager and the Compliance Department.†† The Compliance Department will seek any other necessary approvals pursuant to policy.

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

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

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

Also bear in mind that:

** 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.

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

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

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

If you are a new employee, immediately report any directorships in accordance with the above requirements, and seek approval where necessary. If you change your role within Scotiabank, advise your new Manager of any directorships, even if they were previously approved. He or she can decide whether those approvals must be reconfirmed, given your new duties.

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

f. Wills, Other Trusteeships and Similar Appointments

Customers sometimes try to express appreciation to employees through legacies, bequests or appointments in their wills. You should discourage any customer who suggests making you a gift in their will, as this could create a perception that you manipulated or took advantage of the customer. Except as noted below, you should never solicit from, or accept a personal appointment by, a customer as an executor, administrator or trustee, unless it is within your own family.

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

g. Purchasing Scotiabank Assets or Administered or Repossessed Property

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

- > the purchase is made at an advertised public auction; or
- > it has otherwise been established to Scotiabank's satisfaction that the price being paid is reasonable and your supervising office or department head has approved the transaction; or
- > the purchase accords with an approved Scotiabank program.

Similarly, neither you nor your family are to use or purchase goods that have been repossessed by Scotiabank, except with the permission of your supervising office or department head. They will review the situation and consider whether the transaction would both be, and appear to be, fair.^{§§}

^{§§} If you work for a securities subsidiary, or any other subsidiary or area where a [fiduciary](#) obligation is imposed by law, you may not use or become the owner of property held in fiduciary accounts under administration, unless you or a family member are a beneficiary or co-trustee of an estate and the governing document specifically permits you to use or become the owner of the property being administered.

h. Related Parties

Directors, certain senior officers, their spouses and minor children, as well as certain other entities such as companies which they control, are legally called “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.

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

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 having been thought to have improved Scotiabank’s position at the expense of a customer.
Scotiabank is asked to lead financings for more than one customer’s bid for the same asset.	Risk of having been thought to have given one customer favorable treatment over another, or to have passed information to a customer’s competitor.

Conduct Yourself Honestly and with Integrity

Because customers want to be served by people who are trustworthy and reliable, our success depends on the honesty and integrity of Scotiabank directors, officers and employees. Always remember that your conduct has a direct effect on how customers think about Scotiabank.

I. Illegal or Fraudulent Activities

a. Misappropriation

Stealing customer or Scotiabank funds, attempting to defraud a customer or Scotiabank, or colluding with or knowingly helping others to do so are grounds for termination with cause and possible civil or criminal liability. This includes, but is not limited to, falsifying your expense claims, misuse of employee benefits such as employee banking privileges and corporate credit cards, or misusing Scotiabank's clearing or payments systems or General Ledger accounts to obtain credit or funds not rightfully yours, as for example, by [cheque kiting](#).

b. Improperly Accessing Records, Funds or Facilities

Never use your access to Scotiabank funds or facilities to do something you shouldn't. 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.

c. Creating False Records

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

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

d. Bribes, Payoffs and Corrupt Practices

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

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

For additional guidance on Scotiabank's policies with respect to the prevention of bribery and corruption, refer to the *Scotiabank Anti-Corruption Policy and Guidance* ("Anti-Corruption

Policy”). You may also contact business.conduct@scotiabank.com for further advice or guidance.

e. **Insider Trading and Tipping**

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

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.^{***}

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.

You also may not pass on (or “tip”) inside information about Scotiabank or any other public company to anyone except those persons who need to know that specific information in the necessary course of business.

Employees likely to encounter inside information should become familiar with the specific policies and procedures that the Bank 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**

Directors, officers and employees of Scotiabank are prohibited under provisions of the *Bank Act* from trading in puts or calls of The Bank of Nova Scotia (“BNS”) shares.

Additionally, you may only short BNS shares in strictly limited circumstances provided under the *Bank Act*. See *Scotiabank Group Insider Trading and Reporting Policy* for further guidance.

.g. **Requirement to Disclose a Criminal Charge or Conviction**

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

^{***} Where permitted by the Compliance Department, sales and trading staff may continue to accept unsolicited orders from clients.

h. Illegal or Anti-Competitive Sales Practices

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

Do not collude or co-operate with any other institution in anti-competitive activities. These include arrangements for or discussions about interest rates on loans and deposits, service fees, other product features or types or classes of persons to whom services will be made available or withheld.^{†††}

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

Coercive Tied Selling:

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

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

II. Improper Transaction Prevention

a. Know Your Customer/Understand Your Customer's Transaction

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

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

b. Detecting and Reporting Suspicious or Improper Transactions

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

^{†††} Note: Some permitted exceptions are discussions regarding syndicated loans, underwritings and other kinds of authorized consortia, and certain government lending programs. In these cases, limit discussions to the specific transaction or program.

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

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

- > the gift is modest and would not affect the recipient's objectivity;
- > there is no suggestion that the donor is trying to obligate or improperly influence the recipient;
- > offering or accepting is "normal business practice" for the purposes of courtesy and good business relations;
- > offering or accepting is legal and consistent with generally understood ethical standards;
- > neither you nor Scotiabank would be embarrassed if the public became aware of the circumstances of the gift or entertainment; and
- > it is not a gift or prize of cash, bonds, negotiable securities, personal loans, or other valuable items (such as airline tickets for your personal use, or use of a vacation property).

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

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

- > You may not use your position for improper personal gain. Tactfully

Examples of the types of gifts and entertainment that are acceptable to offer or accept include:

- > occasional meals, refreshments, invitations to local sports, theatre or similar 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.

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

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, you may accept it on behalf of Scotiabank. In these cases, immediately report the gift to your Manager who will advise you how to deal with it. Such gifts may not be taken for your personal use or enjoyment.

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

- > Be especially careful when offering gifts or entertainment to government officials and public office holders (“public officials”). Many countries have strict laws regarding offering anything of value to these individuals.
- > Always comply with the *Anti-Corruption Policy* in any dealings with public officials. Gifts to, or entertainment of, public officials in the amount of US\$100 or above will require additional approvals as set out in the *Anti-Corruption Policy*.

b. **Dealing Ethically with Our Customers and Others**

As Scotiabankers, we do not compromise our ethics for the sake of meeting our sales, profit or other targets or goals.

Steering a customer to an inappropriate or unnecessary product harms the customer, damages our reputation and may be illegal in certain situations and jurisdictions. Never take unfair advantage of anyone through manipulation, concealment, abuse of confidential business or personal information, misrepresentation of material facts, or any other unfair-dealing or unethical business practice.

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

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

c. **Respect Intellectual Property Rights**

When using supplier or service provider and third party systems and programs, comply with the licensing, confidentiality and registration requirements. Failure to do so could subject you or Scotiabank to serious penalties. When using the Internet, always comply with the *Internet and Electronic Mail Code of Conduct*, which contains specific guidance on respecting intellectual property laws.

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

⁺⁺⁺ 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 outsourcing arrangements or other strategic alliances. If you are authorized to engage third parties, you should engage only those who are competent and reputable, and who have business conduct standards comparable to our own, as these are critical considerations for Scotiabank.

V. Communications and Representations

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

a. Advertising

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

b. Proper Public Disclosure

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

c. Making Public Statements and Media Contact

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

Sometimes employees are asked to give presentations or express views on matters generally relating to banking or other financial services, usually due to their position with Scotiabank or acknowledged expertise. Unless you are presenting an official Scotiabank position, make it clear in your presentation that the views expressed are personal and do not necessarily represent those of Scotiabank.

d. Expressing Your Personal Views

As a private citizen, you are entitled to express your personal views. However, be careful not to give the impression that you are speaking on behalf of Scotiabank or expressing Scotiabank's perspective, unless you have obtained approval from your Manager and/or an authorized

spokesperson. This applies to all forms of communication (such as statements, speeches, letters or articles) and all communications media or networks (such as newspaper, radio, television, E-mail 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 internet “blogs”, chat rooms, newsgroups and social networking websites) and refrain from disparaging competitors or making statements that might discredit Scotiabank or its products and services. Also, take particular care not to disclose confidential information about Scotiabank, customers, employees or others.

e. Use of the Scotiabank Brand, Name and Reputation

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

VI. Cooperate with Audits and Investigations

Always cooperate fully with any investigations by management or the Compliance, Internal Audit, Security and Investigation or Human Resource Departments. Be straightforward, candid and truthful when dealing with internal 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 an audit or a legal or governmental investigation.

Respect 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 Confidential Information

Customers, employees, suppliers, service providers and others trust Scotiabank to keep their [personal information](#) and confidential business information safe and secure. For this reason, protecting their privacy and the confidentiality of their dealings with us is essential to safeguarding our reputation. In most instances, maintaining confidentiality is also a local legal or regulatory requirement.

You are expected to be aware of, and follow, the policies and procedures that Scotiabank has put in place to protect confidential information and to comply with applicable laws and regulations.

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

b. Appropriate Handling of Confidential Information

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

Appropriate handling of confidential information includes the following:

- > Follow policies, procedures and processes for storing and controlling access to confidential information, whether stored electronically or as physical documents.
- > Follow the *Internet and Electronic Mail Code of Conduct* and any other policies, procedures or processes for transmitting confidential information including via non-secure media such as fax, E-mail or the Internet.
- > Do not carelessly display confidential information (by, for example, leaving it visible on a computer monitor in a public space, or leaving confidential documents lying about in an unsecured manner where they could be viewed, lost or stolen).
- > Do not disclose confidential information to persons outside Scotiabank (including family or household members or close associates) or to other employees who do not require the information for their work.
- > Take care when discussing confidential information where it might be overheard or intercepted (such as when using a cell phone) by, for example, being certain to whom you are speaking and ensuring that your conversation cannot be overheard by unauthorized persons. Never discuss confidential information in social settings, such as restaurants, elevators, trains and other public places.
- > Destroy or dispose of information according to security requirements and policies and procedures for document retention and destruction.

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

Never access customer or employee personal information, or confidential business information about Scotiabank or a customer, without a legitimate business reason and proper authorization.

c. **Disclosures of Confidential Information**

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

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

II. Accuracy and Integrity of Transactions and Records

The expectations of our customers, shareholders, regulators and other stakeholders make it essential that Scotiabank's books and records are complete and accurate. All employees must play their part in ensuring the accuracy and integrity of our record-keeping and information reporting systems. Follow applicable policies, procedures, and processes to ensure that transactions:

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

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

III. Security

a. **Keep Scotiabank and Customer Assets Safe**

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

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

Be careful not to compromise security through the inappropriate disclosure of information or images, such as photographs. Never discuss or disclose the design or operation of systems or security protection processes or procedures with anyone outside or inside Scotiabank, other than on a need-to-know basis.

Report any perceived weakness or deficiency in a system or security protection procedure to your Manager or other appropriate senior officers.

b. Integrity of Computer and Communication Systems

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

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

c. Assets or Information in the Hands of Third Parties

If you have authorized assets or 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.

d. Use of Scotiabank Property and Information Off-Premises

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

- > consider the sensitivity of information before taking it off-premises, whether in hard copy or electronic format, and take only the minimum information required;
- > ensure all confidential information is safeguarded from unauthorized access, theft, misuse, loss or corruption in keeping with applicable policies, procedures and processes; and

- > never copy Scotiabank information for your or someone else's non-work-related use without authorization.

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

e. Appropriate Use of Information Technology and Services

Electronic and telecommunications facilities and systems, such as computers, Internet access, voice mail, E-mail, fax machine and telephone, are provided to you to enable you to do your job. Any other use, except for reasonable and occasional use, is not allowed. Refer to the *Internet and Electronic Mail Code of Conduct* for guidance on the appropriate use of information technology and services, including the Internet, intranet and E-mail.

Treat Everyone Fairly, Equitably, and Professionally, Whether They are Customers, Suppliers or Service Providers, Employees or Others who Deal with Us

Scotiabank is committed to treating all current and potential employees, customers, suppliers, service providers and others who deal with us fairly, and to maintaining a work environment that supports the productivity, personal goals, dignity and self-respect of all employees. This includes commitments to:

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

I. Diversity, Equity and Human Rights

Harassment and Discrimination

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

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

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

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

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

II. Workplace Health and Safety

Scotiabank is committed to providing its employees with a healthy, safe workplace, in compliance with applicable local laws and regulations. This includes a commitment to providing

a workplace that is free from violence by maintaining a respectful, non-threatening work environment.

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

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

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

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 and processes with respect to, for example, environmental credit risk, responsible environmental management of our real estate holdings and enhanced social and environmental guidelines for project finance loans in developing countries.

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

II. Charitable and Community Activities

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

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

III. Political Activities

a. Political Activities and Donations in the Name of Scotiabank

The Bank and certain of its subsidiaries may make political donations, wherever permitted by law, to support and encourage the democratic process as distinct from the fortunes of individual parties. You should direct any political donation requests to the Chief Executive Officer of the Bank or your subsidiary.

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

b. Personal Political Participation

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

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

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

IV. Other Codes of Conduct and Voluntary Commitments

a. Commitments by Scotiabank

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

b. Professional Codes of Conduct

Many professions and professional bodies have codes of conduct or ethics to which they expect their members to adhere. If you come across an instance where your profession's code of conduct conflicts with these Guidelines, inform your Manager and the Compliance Department immediately.

Getting Help or Reporting Problems and Irregularities

I. Obligation to Report

Promptly reporting breaches can help protect both you and Scotiabank, as well as other employees, customers, shareholders and other stakeholders. If you believe that you may have breached the Guidelines, or a supplemental guideline or code of conduct that applies to you, you have an obligation to report it to your Manager immediately. Failing to do so is grounds for termination with cause.

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

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

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

II. Protection from Retaliation

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

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

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

III. How to Report

a. Pathways to Resolution Guide

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

their local Human Resources Call Centre, or to their local Human Resources department or representative.

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

b. Alternative, Confidential Avenues

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

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

c. Getting Help or Advice

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

Glossary [\[Back to Overview\]](#)

Bank means The Bank of Nova Scotia. [\[back\]](#)

Board of Directors means the Board of Directors of The Bank of Nova Scotia. [\[back\]](#)

Cheque kiting is fraudulently obtaining unauthorized credit by writing a cheque against an account with insufficient funds, and making up the deficiency by depositing another cheque from a different bank account which may or may not have funds. [\[back\]](#)

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

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

[\[back\]](#)

Compliance Department means Scotiabank Global Compliance, including Global Compliance Executive Offices (Toronto), and local and subsidiary Compliance departments. [\[back\]](#)

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

Confidential information comprises customer or employee personal information, confidential business information and any other information about Scotiabank or another business that has not been generally disclosed to the public. See also "personal information" and "confidential business information." [\[back\]](#)

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

Employees means full-time, part-time and temporary or contract employees of The Bank of Nova Scotia and its global subsidiaries. "Employees" may also include certain independent contractors who, while not technically employees within the meaning of applicable labour or tax laws, have been identified by Compliance as being subject to the Scotiabank Guidelines for Business Conduct. [\[back\]](#)

A **fiduciary** is someone who has undertaken to act for the benefit of another and is in a position of trust. [\[back\]](#)

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

Inside information is material information that has not been generally disclosed to the public. See also “material information”. [\[back\]](#)

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.” [\[back\]](#)

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 the Bank or a subsidiary is or has agreed to be bound. [\[back\]](#)

Legal Department means your local or subsidiary Legal Department, or Legal Department Executive Offices (Toronto). [\[back\]](#)

Manager means your branch manager, department manager, supervisor or unit head. See also the “*Pathways to Resolution*” guide. [\[back\]](#)

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. [\[back\]](#)

Money laundering is defined as the process of concealing the existence, illegal source, or application of income derived from criminal activity, and the subsequent disguising of the source of that income to make it appear legitimate. [\[back\]](#)

Pathways to Resolution guide means the Bank’s published guide, “*Pathways to Resolution*”. Subsidiary employees should read this and words such as “Manager”, “department head” or “supervising office” in the context of their subsidiary’s organizational structure and escalation processes. [\[back\]](#)

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

Personal information does not include the name, title, business address or telephone number of an employee of Scotiabank. All other information about or received from individual customers or employees should be presumed to be personal information unless the contrary is clear. [\[back\]](#)

Policies, procedures, and processes refer to all applicable manuals, handbooks, job aids, forms, policies, practices, procedures, processes, standards, programs and requirements as implemented by the Bank or a subsidiary. [\[back\]](#)

Scotiabank refers to The Bank of Nova Scotia and all of its subsidiaries. [\[back\]](#)

Subsidiaries means subsidiaries of The Bank of Nova Scotia. [\[back\]](#)

Terrorist financing means using, transferring, transmitting or dealing with funds or property intended to support terrorist activities. [\[back\]](#)

Tipping is passing “inside information” about a company to another person, except where the conveyance of the information is in the necessary course of business. See “inside information” and “insider trading”. [\[back\]](#)