

## **Scotiabank's Whistleblower Program**

The Bank of Nova Scotia (the "Bank") has established channels through which employees and external parties can raise a concern to ensure that matters are reported and addressed. The Whistleblower Program is part of the larger Raise a Concern framework. The Whistleblower Program is designed as a control to safeguard the integrity of the Bank and its subsidiaries, its financial reporting, and its business dealings and to support adherence to the Scotiabank Code of Conduct (the "Code") and its regulatory obligations. The Whistleblower Program enables employees and other parties to raise concerns through a confidential channel, hosted by an independent third-party provider, and to proceed anonymously if they wish. The Whistleblower Program enables employees and other parties to raise concerns through a confidential channel, and has oversight of the receipt, assessment, investigation, and resolution of concerns, particularly when those concerns relate to Wrongdoing.

Concerns raised through the Whistleblower Program are taken seriously and reviewed in detail. If the concern is deemed in scope of the Whistleblower Program, an investigation will be conducted, and you will be notified when the matter is considered closed. The Whistleblower Program maintains communication with the reporters who raise their concerns through the EthicsPoint platform and may ask for additional information to look into the concerns. While the level of detail the Bank is at liberty to share post investigation may be impacted by privacy and other considerations, the Bank is committed to updating reporters who raise concerns through this channel.

### **Who Can Report?**

Anyone can file a report through the Whistleblower Program. Employees, vendors and certain third parties are obligated by the [Scotiabank Code of Conduct](#) to report concerns and the Whistleblower Program affords them the opportunity to do so confidentially and anonymously. Clients and members of the public can also raise concerns if they relate to Wrongdoing by a Bank employee, vendor or certain third parties. The Whistleblower Program is not a client complaints channel so concerns of this nature will be redirected to the appropriate channel.

### **What Should be Reported?**

Breaches of the Scotiabank Code of Conduct including:

- Auditing and accounting concerns
- Bribery or corruption
- Improper sales conduct
- Fraud, theft or destruction of property

- Market abuse
- Money laundering, terrorist financing or sanctions violations
- Privacy and confidentiality breaches
- Retaliation for having raised a concern
- Non-compliance with a Bank policy or procedures
- Non-compliance with a requirement under the Bank Act (Canada) other law or its regulations
- Unethical use of data
- Mistreatment (harassment, discrimination)
- Health and safety concerns
- Environmental, social and governance concerns
- Failure to meet a [Public Commitment](#) made by the Bank (e.g., including a commitment communicated in the Global Human Rights Statement)

The Whistleblower Program is not the optimal channel for reporting harassment and discrimination. Employees are encouraged to review the Bank's internal Raise a Concern Policy, reach out to Human Resources, or Employee Relations or seek advice from the Staff Ombuds Office prior to filing a report through the Whistleblower channel.

### **How do I file a report?**

Scotiabank has partnered with a third-party vendor to support the Whistleblower Program. The service is available at: [Scotiabank.EthicsPoint.com](https://Scotiabank.EthicsPoint.com)

The EthicsPoint service will allow you to file your report confidentially online or by telephone. You can also submit a report through your mobile device using this QR Code:



The service is accessible globally 24 hours a day, 7 days a week in multiple language including English, French and Spanish. Additional information about the Whistleblower Program can be found on the Whistleblower internet page.

We ask that Reporters who raise concerns through this channel provide us with adequate detail to support our review. This means including as much information as possible about what happened, where it happened, when it happened, how it happened, who was involved (including potential witnesses to the issue), and your views on why it

may represent a breach of [Code of Conduct](#), or a problem with Scotiabank's policies, procedures, guidelines, process or controls.

It is very important that you remain engaged in the process after submitting the report. We encourage you to log back into EthicsPoint using your report key and password to check for any messages or follow up questions from the Whistleblower Program. This will help us and our investigative partners to look into the matter more quickly and effectively.

Scotiabank does not tolerate Retaliation against any person who raises a concern or participates in an investigation. Allegations of Retaliation are taken seriously and will be addressed promptly.

Notwithstanding the Bank's obligation to protect the anonymity of individuals who raise concerns, there are circumstances where the identity of these individuals, when known, will be shared with regulators at their request or if otherwise required by law or regulation.

Bank employees may report concerns to certain regulators directly without notice to the Bank. For example, in Canada, employees may submit concerns to the [Commissioner of the FCAC](https://www.canada.ca/en/financial-consumer-agency.html) (<https://www.canada.ca/en/financial-consumer-agency.html>) or the [Superintendent of OSFI](https://www.osfi-bsif.gc.ca/en) (<https://www.osfi-bsif.gc.ca/en>). Employees may also contact law enforcement agencies in their jurisdiction where warranted. Individuals reporting concerns to law enforcement or to a regulator will also be afforded protection from Retaliation.

The Whistleblower program is not equipped to address urgent matters related to physical security and immediate dangers to the health and safety of clients, employees or property. Emergencies should be reported to Corporate Security through the Security Operations Centre at 416-866-5050 or [CS.SOC@bns.scotiabank.com](mailto:CS.SOC@bns.scotiabank.com).