Whistleblower Policy

Note

Please speak up if you have concerns about irregular business activities or behaviour that could put CIBC's integrity or reputation at risk. For information on what to report and how to contact us, please see below or visit CIBC's Whistleblower Hotline webpage (internal / external).

Current issue:	May 2021
Availability:	Policy site: Whistleblower Policy
Approved:	Audit Committee
Approval date:	May 26, 2021
Next review:	May 2023

Table of contents

1.0 Summary

CIBC's Code of Conduct ("Code") requires all CIBC team members (collectively all CIBC employees, directors and contingent workers[1]) to speak up if something does not seem right, if they have a concern about their role, activities they believe are inconsistent with the Code, or something that might be damaging to CIBC or our stakeholders. In addition, third parties such as CIBC suppliers or clients may want to report questionable or unethical conduct they observe in relation to CIBC.

Whistleblowing refers to notifying CIBC of any irregular business activities or behaviour that could put CIBC's integrity or reputation at risk or that is otherwise reportable under applicable whistleblower legislation.

This Whistleblower Policy ("Policy") supplements the Code and provides a framework to facilitate individuals in reporting their concerns to CIBC, anonymously if required, and without fear of retaliation. The Policy also provides information about how such reports are handled by CIBC and other activities associated with administering the Policy (collectively, the "Whistleblower Program").

2.0 Intent

The intent of this Policy is to:

- encourage escalation of concerns regarding questionable or unethical conduct;
- support adherence to the Code and deter wrongdoing;
- ensure compliance with legal and regulatory requirements[2] regarding whistleblowing;
- ensure the integrity of CIBC's accounting, internal accounting controls, auditing and financial reporting; and
- protect CIBC's reputation.

3.0 Audience and Scope

The Policy applies to Canadian Imperial Bank of Commerce and, subject to review and approval where required by applicable law, its wholly-owned subsidiaries[3] (collectively "CIBC") and must be followed by all CIBC team members.

Region-specific information and accountabilities are set out in the Appendices. In addition, certain regions and / or lines of business ("LOBs") may have whistleblower policies or procedures in place that include requirements that are in addition to the requirements set out in this Policy. Team members are responsible for ensuring that they are aware of any of these additional requirements applicable to them.

Contravention of any provision of this Policy by an employee may result in disciplinary action up to and including termination of employment for cause, without notice or pay in lieu of notice, as well as possible civil, criminal or regulatory action. Such conduct may also affect individual performance assessment and compensation.

Contravention of any provision of this Policy by a contingent worker may result in action by CIBC up to and including termination of the individual's assignment without notice, as well as possible civil, criminal or regulatory action.

---

1 Temporary agency workers, contractors and service provider workers providing support to CIBC.

2 "Regulatory requirement" is defined in the Regulatory Compliance Management Policy.

3 Controlled- subsidiaries, joint ventures in which CIBC is a partner and certain other CIBC legal entities operate in an autonomous manner. They are expected to develop their policies, where applicable, in a manner consistent with this document.

4.0 Policy Requirements

4.1. Requirement to Report Concerns to CIBC

4.1.1. What Types of Concerns to Report

CIBC team members must report concerns regarding irregular business activities or behaviours that could pose reputational risk to CIBC or are reportable under applicable whistleblower legislation. Generally, this refers to concerns that involve:

- accounting, internal accounting controls, financial reporting, or auditing matters;
- dishonesty by CIBC team members or other third parties with the intent to deceive or steal from CIBC, its team members, clients or shareholders (e.g. theft of assets, misstatement of financial reports, bribery, kickbacks, and theft of information);
- activity that may be an indication of fraud (e.g. abnormal patterns of employee behaviour, intentionally disregarding controls and suspicious lending patterns);
- unauthorized disclosure of confidential information about CIBC, its clients or suppliers; and
- actual or potential retaliation as a result of reporting a concern, or for assisting in an investigation.

Note

For other types of concerns, individuals should first consult the Code (and other relevant CIBC policies) to identify the most appropriate reporting method. For example, CIBC Employee Relations can be engaged to assist with workplace or peer-to-peer complaints, Client Care can be contacted to resolve customer service issues etc.

4.1.2. Options for Reporting a Concern

Note

CIBC offers a variety of secure, professional and simple mechanisms (outlined below) to ensure team members and third parties can speak up about concerns they may have. The most up-to-date contact information can be found on CIBC's Whistleblower Hotline webpage (internal / external).

4.1.3. Whistleblower Hotline (phone and web portal)

CIBC's Whistleblower Hotline can be accessed by phone or online and is:

- Operated by an independent company, outside of CIBC, available 24 hours a day, 7 days a week and in multiple languages (upon request).
- No identifying information (including a user’s name or telephone number) is available to the service provider.
- Users can choose to provide contact information for CIBC to contact them directly or they can choose to remain anonymous. Anonymous users are provided with a unique key to access their report and updates or questions from CIBC at a later time.
- For hotline calls, CIBC receives a written transcript only. While calls may be monitored by the service provider for quality control or training purposes, they are not recorded.

4.1.4. Email / Mail

The Whistleblower Program and certain groups within CIBC (e.g. Corporate Security) can be contacted directly at any time to report concerns. Executives, such as CIBC's Chief Executive Officer and members of CIBC's Executive Committee ("ExCo") and Board can be advised of concerns by writing to the CIBC Corporate Secretary (and their regional counterparts outside of Canada).

Note

In accordance with section 5.0 below, all information received by the Whistleblower Program will be treated confidentially to the extent possible and in a manner consistent with CIBC's responsibility to address the issue raised and in accordance with applicable whistleblower legislation.

4.2. Requirement to Protect Individuals from Retaliation

As set out in the Code, no one may suspend, discharge, discriminate against, harass, or threaten, in any manner, or otherwise retaliate against a team member or other person in any way for:

- reporting in good faith actual or possible misconduct; or
- providing information for, or participating in, an investigation.

Nothing in the Code, any policy, or any agreement entered into with CIBC, prevents a team member from engaging in activities permitted by whistleblower legislation. CIBC takes steps to detect and protect against retaliation, including:

- assessment of concerns reported for implicit or explicit indications of retaliation;
- escalation to appropriate groups (e.g. CIBC Legal) where a risk of retaliation is identified;
- providing multiple independent methods for alerting CIBC to instances of actual retaliation;
- ongoing / follow-up communications sent (if a means to contact are provided to CIBC) to ensure retaliation has not occurred;
- periodic review of outcomes for team members who identified themselves in the course of reporting their concerns; and
- providing support services for team members (e.g. Employee Assistance Program).

Note

If you believe that you are being retaliated against you should let CIBC know immediately. Please refer to CIBC's Whistleblower Hotline webpage (internal / external) for contact information.

4.3. Requirement to Independently Review Concerns

All information received in accordance with this Policy is independently reviewed by Privacy Office ("Privacy") and assigned to an appropriate party for investigation in accordance with established Whistleblower Program procedures. The Whistleblower Program procedures also detail instances where Privacy may notify or engage other relevant parties for notification or guidance purposes (e.g. reporting of allegations of actual or potential regulatory non-compliance to Enterprise-wide Compliance etc.).

CIBC will appropriately investigate and address all reports made in good faith in a timely manner, however:

- the length of time to complete an investigation will vary based on the complexity of the concern reported and investigation required; and
- CIBC may be unable to effectively investigate or address concerns where the information provided to / available to CIBC is insufficient or vague.

CIBC will attempt to contact whistleblowers who have provided contact information to provide updates (e.g. to acknowledge receipt of a concern, request clarification / additional information (if necessary) and advise when an investigation has been completed). For privacy reasons, CIBC is unable to provide specific details of an investigation, including the outcome.

Once an investigation has concluded, the findings and recommendations for closure are independently reviewed (and approved where appropriate) by Privacy. This information is documented and reported to those responsible for oversight in accordance with section 6.0.

Note

In accordance with the Policy, CIBC will appropriately investigate all concerns reported in good faith, regardless of whether the information provided qualifies for legal whistleblower protection or not.

4.4. Significant concerns

If Privacy determines that a concern reported in accordance with this Policy contains allegations that pose potentially significant risk, including regulatory or reputational risk, to CIBC ("Significant Concerns"), Privacy will notify the Vice-President and Associate General Counsel (Ombudsman & Privacy) ("Vice President – Privacy") immediately[4]. The Vice President – Privacy may notify representatives of senior management and any other representatives and/or the Audit Committee as deemed appropriate. The Vice President – Privacy may also engage an independent third-party as appropriate to advise on the investigation and resolution of any Significant Concern.

4.5. Requirement to Protect Anonymity and Confidentiality

CIBC takes steps to protect the anonymity of individuals and the confidentiality of the concerns they report to CIBC, including:

- strictly limiting access to all information received through whistleblower reporting mechanisms to those directly involved in managing and investigating the concerns raised;
- ensuring information received is handled and investigated by qualified team members;
- securely storing all paper and electronic documents and other materials relating to whistleblower reports;
- limiting the dissemination of personal / identifying information as much as possible (e.g. redaction); and
- ensuring all team members, including those involved in handling and investigating information received through whistleblower channels are bound by CIBC's Code and policies on confidentiality.

[4] If a Significant Concern contains an allegation involving the Vice President - Privacy, Privacy will directly notify a representative of senior management in Corporate Security or Human Resources.

4.6. Requirement to Treat Individuals Fairly

In accordance with legal and regulatory obligations, CIBC also takes steps to ensure that all individuals mentioned in, or the subject of, concerns / information reported in accordance with this Policy are treated fairly, including:

- objective, fair and independent investigation process (e.g. conflicts are outsourced internally / externally where identified);
- independent review of investigation outcomes by Privacy;
- the objective of an investigation is to determine whether there is enough evidence to substantiate or refute the matters reported;
- determining facts and gathering evidence without notifying an implicated team member or their manager as far as possible;
- advising an implicated team member as and when required by principles of natural justice and procedural fairness and prior to any actions being taken; and
- providing support services for all team members (e.g. Employee Assistance Program).

4.7. Management Reporting Requirements

4.7.1. Audit committee

Privacy will report the results of CIBC's whistleblowing program to the Audit Committee comprising:

- accounting, internal accounting controls or auditing matters reported in accordance with the Policy;
- the status and outcome of all concerns raised through the Whistleblower Hotline, managed by Privacy under the Policy, and any concerns raised in accordance with regional whistleblower policies;
- the outcome of any root-cause analysis conducted on themes or trends identified among substantiated concerns;
- concerns that were raised in accordance with the Policy regarding Executives (Vice President (or equivalent) or above) that result in some form of disciplinary outcome beyond coaching; and
- management reports on the procedures established for the receipt, retention and treatment of complaints received by CIBC from team members or third parties, confidentially and anonymously, regarding accounting, internal accounting controls, or auditing matters.

4.7.2. External auditors

On a quarterly basis, Privacy will report to CIBC's external auditors on all accounting, internal accounting controls or auditing matters reported in accordance with the Policy.

5.0 Monitoring and oversight

Whistleblowing regulatory requirements and this Policy are subject to the following monitoring and oversight mechanisms:

- management reporting to the Audit Committee in accordance with section 4.7 above;
- the procedures in place to support the receipt, retention and treatment of concerns received by CIBC in accordance with section 8.2 below; and
- testing for compliance with the requirements of the Policy, conducted as part of the testing programs administered by groups including Risk Management and Internal Audit.

6.0 Accountabilities

Note

This section outlines the main activities associated with the Whistleblower Program by Privacy and associated groups in Canada. For additional accountabilities specific to certain regions, please refer to the Appendices.

6.1. CIBC Team Members

All CIBC team members must comply with this Policy and promptly report concerns about irregular business activities or behaviour that could put CIBC's integrity or reputation at risk in accordance with section 3.0 above.

6.2. Privacy Office

The Privacy Office ("Privacy") is responsible for overseeing the operation CIBC's Whistleblower Program on an enterprise-wide basis, which in turn assists the Audit Committee in discharging certain responsibilities in the Audit Committee mandate.

Specifically, Privacy is responsible for:

- establishing Whistleblower Program procedures for the receipt, retention and treatment of concerns reported in accordance with the Policy;
- immediately escalating any Significant Concerns in accordance with Section 4.4;
- assigning and tracking investigations of concerns reported in accordance with the Policy and Whistleblower Program procedures as required;
- approving closure of all such investigations (other than those assigned to Human Resources for investigation);
- reporting to the Audit Committee and CIBC's external auditors in accordance with section 6.0 above;
- providing US Region with a reconciliation of US-related matters for reporting on a quarterly basis and upon request;
- retaining initial report of concerns received in accordance with the Policy, together with the outcome of investigations of such concerns, in accordance with the Records Management Policy[5];
- overseeing the activities of the Whistleblower Hotline third-party supplier;
- maintaining and updating this Policy in accordance with section 7.0 below;
- providing advice and guidance regarding this Policy; and
- monitoring and communicating whistleblowing regulatory requirement changes to relevant LOBs on a timely basis.

[5] The Records Management Policy is not applicable to CIBC Bank USA as of November 1, 2018. In the meantime, please refer to the Code of Conduct CIBC Connect site to review the applicable CIBC Bank USA policies.

6.3. Audit Committee

The Audit Committee shall:

- review the results of CIBC's whistleblowing program;
- ensure procedures are established for the receipt, retention and treatment of complaints received by CIBC from team members or third parties, confidentially and anonymously, regarding accounting, internal accounting controls, or auditing matters; and
- review management reports on the procedures and investigations.

6.4. Corporate Security

Corporate Security shall:

- investigate concerns assigned to Corporate Security under this Policy and report outcomes to Privacy on a quarterly basis;
- inform Privacy and Finance of any concerns regarding accounting, internal accounting controls or auditing matters reported to Corporate Security; and
- inform Privacy of any other concerns reported to Corporate Security that involve an allegation of retaliation or an express or implied fear of retaliation as a result of reporting a concern, or for assisting in an investigation.

6.5. Finance

Finance is responsible for supporting Corporate Security in their investigations of concerns regarding accounting, internal accounting controls or auditing matters, as requested by Corporate Security

6.6. Human Resources

Human Resources shall:

- immediately inform Corporate Security of any concerns reported to Human Resources regarding accounting, internal accounting controls or auditing matters;
- investigate concerns assigned to Human Resources under this Policy and report outcomes to Privacy on a quarterly basis; and
- inform Privacy on a quarterly basis of any concerns reported to Human Resources under this Policy regarding Executives that result in some form of disciplinary outcome beyond coaching.

6.7. Fraud Management

Fraud Management shall:

- investigate concerns assigned to Fraud Management under this Policy and report outcomes to Privacy on a quarterly basis.

6.8. Other Groups

The following groups shall immediately advise Corporate Security when they receive reports of concerns regarding accounting, internal accounting controls or auditing matters:

- Client Care
- Ombudsman's Office
- Corporate Services
- Corporate Secretary

7.0 Maintenance and review

The Executive Vice-President and Chief Legal Officer is the ExCo sponsor of this Policy and has delegated - ownership and recommendation of approval to the Vice President - Privacy. The Vice President - Privacy is responsible for the development, implementation, maintenance, review and recommending approval of this Policy.

This Policy will be reviewed every two years, and will be revised if necessary. The review and any substantive revisions will be submitted to the Audit Committee for approval. Non-material, interim changes may be approved by the Vice President, Privacy.

The Policy was approved by the Audit Committee on [May 26], 2021. The next full review will be in May 2023.

8.0 Related materials

- Code of Conduct
- Whistleblower Hotline webpages (internal / external)
- Records Management Policy
- Supplier Code of Conduct

Appendix A – Australia

Purpose

This Appendix A provides supplementary information for individuals located in Australia. It is intended to satisfy the requirements for whistleblower policies set out in the Australian Corporations Act 2001, as amended. In the event of a conflict between Appendix A and the Policy in Australia, Appendix A prevails.

Qualifying for Legal Protection as a Whistleblower in Australia

To qualify for legal protection as a whistleblower under Australian law, you must meet 3 criteria:

1. **You must be a whistleblower in relation to CIBC.** This means you are a current or former CIBC:
    - officer or employee;
    - supplier or supplier employee (whether paid or unpaid);
    - associate; or
    - a relative, dependent or spouse of an individual listed above.
2. **Your concern must be about certain types of misconduct.** For clarity, this may include:
    - illegal conduct (e.g. fraud, theft, violence or breaches of Australian securities or banking laws or regulations); or
    - conduct that is not unlawful but indicates a systemic issue or an improper state of affairs (e.g. business behaviour and practices that may cause consumer harm, a danger to the public or the financial system).

Reporting such misconduct qualifies for protection under Australian law even if your allegations turn out to be incorrect.

Conversely, Australian law provides no whistleblower protection for reporting other types of concerns, such as:

- purely personal work-related grievances (e.g. interpersonal conflicts at work); or
- violations of the CIBC Code or policies that are not illegal, systemic in nature or have harmful impacts outside of CIBC.

Note

In accordance with the Policy, CIBC will appropriately investigate all concerns reported in good faith, regardless of whether the information provided qualifies for legal protection in Australia or not.

3. **You must report your concern directly to certain individuals.** Individuals authorized to receive a CIBC whistleblower report (anonymously or otherwise) may be:
    - designated by CIBC (see applicable methods in section 4.1 – Reporting Concerns, the internal / external Whistleblower Hotline webpages, and the Australia-specific contact information below); or
    - external to CIBC (e.g. legal practitioners[6] and regulatory bodies (such as ASIC, APRA or the ATO) or, in certain circumstances[7], parliamentarians and journalists).

[6] Reporting a concern to a legal practitioner for the purposes of obtaining legal advice or legal representation regarding the operation of the whistleblower provisions in the Corporations Act are protected even if the legal practitioner concludes that the concern is not about a type of misconduct that qualifies for legal protection.

[7] Legal protection applies whether concerns are reported internally (using CIBC's designated whistleblower channels) or externally, however there are important criteria for making public interest and emergency disclosures set out in the Corporations Act.

Contact Information for Reporting a Concern in Australia

- **Human Resources** – in your regional office (Asia, Pacific and Caribbean)
- **Corporate Security** – Corporate Security, Mailbox
- **Whistleblower Program** – Whistleblower, Mailbox
- **Whistleblower Hotline** – by phone: 1300-849-145 or online (go to www.clearviewconnects.com, click "Submit a Report" and search for CIBC).
- In addition, whistleblowers in Australia may report concerns to internal or external auditor (including a member of an audit team conducting an audit) or an actuary of CIBC.

Note

Contact information may change from time to time. Please visit CIBC's Whistleblower Hotline webpage (internal / external) to confirm the most up-to-date contact information.

Individuals requiring additional information prior to raising their concern may contact Whistleblower, Mailbox for assistance.

Legal Protections Available to Whistleblowers in Australia

Whistleblowers in Australia are legally protected in various ways. For example, it is illegal in Australia (except in limited circumstances) for a person to identify a whistleblower, or disclose information that is likely to lead to their identification. It is also illegal to retaliate against a whistleblower in Australia. See sections 4.3 – Investigation and 4.2 – Retaliation, above, for further information regarding the practical steps CIBC takes to ensure whistleblowers remain protected.

Under Australian law, a person can also seek compensation and other remedies through the courts if they suffer loss, damage or injury for whistleblowing caused by a failure to take reasonable steps to prevent retaliation. Australian law also protects whistleblowers from civil, criminal and administrative liability in relation to their whistleblowing. However, this does not grant immunity for any misconduct engaged in by the whistleblower that is revealed by their whistleblowing.

Links to Related Materials & Policies

The Whistleblower Policy is available to CIBC team members via CIBC Today and is available to third parties upon request by emailing Whistleblower, Mailbox. CIBC's WB Policy may also be referenced by CIBC team members from the CIBC Code of Conduct and within mandatory annual training modules.

The Whistleblower Hotline webpages are available both internally and externally.

Appendix B – Luxembourg

Purpose

This Appendix B provides supplementary information for individuals located in Luxembourg, including team members of CIBC Capital Markets (Europe) S.A. (CIBC Europe). It is intended to satisfy the provisions set forth by the Commission de Surveillance du Secteur Financier (CSSF) Circular 12/552, as amended and by the AML/CFT law dated 25 March 2020. In the event of a conflict between Appendix B and the Policy in Luxembourg, Appendix B prevails.

This Appendix B becomes effective upon formal approval by the CIBC Europe Board of Directors and will be reviewed on a bi-annual basis at least or when required by major changes in the Bank (internal governance framework) and operational processes of CIBC Europe and affiliated entities. Any amendments will be formally reviewed by CIBC Europe management and formally approved by the CIBC Europe Board of Directors.

Contact Information for Reporting a Concern in Luxembourg

The Whistleblower Hotline webpage sets out different methods for reporting concerns, including:

- **Corporate Security** – Corporate Security, Mailbox
- **Whistleblower Program** – Whistleblower, Mailbox
- **Whistleblower Hotline** – by phone: 800-24-626 or online (go to www.clearviewconnects.com, click "Submit a Report" and search for CIBC).

Individuals in Luxembourg may also report their concerns directly to CIBC Europe's Chief Compliance Officer or any Director of the CIBC Europe Board of Directors. Additionally, concerns can be reported to the CSSF or to any local authority (e.g. Financial Intelligence Unit, Ministry of Finance (FIU)) at any time (even without first initiating an internal report):

- CSSF Whistleblowing procedure
- CSSF Whistleblowing Form

Note

Contact information may be updated from time to time. Please visit CIBC's Whistleblower Hotline webpage (internal / external) to confirm the most up-to-date contact information and contact Whistleblower, Mailbox if further assistance is required.

Accountabilities

For clarity, in addition to the accountabilities set out in section 6.0, above:

- Privacy Office and CIBC Europe shall notify each other of concerns reported to ensure appropriate tracking and investigation / handling.
- CIBC Europe management shall be responsible for ensuring investigation outcomes are reported to the corresponding body (CIBC Europe management and Board of Directors or CSSF) to take corrective actions when applicable. Upon receipt of the whistleblowing concern, initial assessment will be made by the CCO and will then contact the relevant CIBC case officer. The case officer will be informed of any escalations so far and any immediate decisions / actions taken.
- Should the concern involve AML/CFT, the primary authority that needs to be informed in Luxembourg is the local FIU and in the case of sanctions, the Ministry of Finance.

- The CIBC Europe Annual Compliance Report will need to include any whistleblowing report pertaining to Luxembourg.

The whistleblower will be informed in writing that their concern will be considered and escalated as appropriate.

Appendix C – United Kingdom

For information about whistleblowing in the United Kingdom, refer to the Speak Up Policy (United Kingdom).

Appendix D – United States of America

Purpose

This Appendix D provides supplementary information for individuals located in United States of America ("USA" or "US"), including employees of CIBC Bancorp USA Inc. and its consolidating subsidiaries (including, without limitation, CIBC Bank USA, CIBC National Trust Company, CIBC Private Wealth Advisors, Inc. CIBC Delaware Trust Company, CIBC World Markets Corp. and CIBC Inc.) as well as the US branch(es) of Canadian Imperial Bank of Commerce, collectively referred to as the combined US operations ("CUSO"). It is intended to satisfy the provisions set forth by the US Standards Relating to Audit Committees (as added by Section 301 of the Sarbanes-Oxley Act of 2002), US Whistleblower Sections 1513 (e), 1514A, 1514A (a) (1), 1514A (a) (2), 1514A (a) (b), Interpretation of the SEC's Whistleblower Rules Under Section 21F of the Securities Exchange Act of 1934 (17 CFR 241), Securities Whistleblower Incentives and Protections (17 CFR 202.12, 17 CFR 205.1, 17 CFR 205.3, 17 CFR 243, 17 CFR 248), and US Dodd-Frank Non-retaliation Section 922. In the event of a conflict between Appendix D and the Policy, Appendix D prevails.

This Appendix D becomes effective upon review by CUSO management and acknowledgement by the CIBC Bancorp USA Inc. Board of Directors ("US Board"). This Appendix will be reviewed on a biannual basis at least or when required by major changes in the Bank (internal governance framework) and operational processes of CUSO.

Contact Information for Reporting a Concern in the US

As noted in Section 3.2, CIBC offers a variety mechanisms for reporting irregular business activities or behaviour on its Whistleblower Hotline webpage (internal / external). For convenience, the contact information most relevant for individuals located in the US wishing to report concerns through whistleblower and other channels is listed below.

- **Human Resources (US)** – by emailing HR@cibc.com
- **Corporate Security** – by emailing Corporate Security, Mailbox
- **Whistleblower Program** – by emailing USWhistleblower, Mailbox
- **Whistleblower Hotline** by phone: 1 866 881-9430 or online (go to www.clearviewconnects.com, click "Submit a Report" and search for CIBC).
- **Contact any member of the US Region Executive Committee, or any member of the U.S. Board** – by writing to the US Corporate Secretary at 120 South LaSalle Street, Suite 400, Chicago, Illinois 60603 USA.

Note

While every effort is made to ensure accuracy, contact information may be updated from time to time. Please see CIBC's Whistleblower Hotline webpage (internal / external) for the most up-to-date contact information. Contact Whistleblower, Mailbox if further assistance is required.

The US Conduct and Culture Risk team is responsible for overseeing the operation of Whistleblower Program functions in the US Region. The Audit Committee of the CIBC Bancorp USA, Inc. Board of Directors ("US Audit Committee") executes certain responsibilities under this Policy / Appendix D as discharged by the Audit Committee of the CIBC Board of Directors.

Significant Concerns

In the event that US Conduct and Culture Risk determines that a concern contains allegations of a Significant Concern, US Conduct and Culture Risk will immediately assess the Significant Concern with Privacy (who will in turn follow Section 5.2) and notify the US Chief Compliance Officer ("CCO") and the US Chief Risk Officer ("CRO") – US Region of the Significant Concern shortly thereafter[8].

The US CRO and US CCO may notify representatives of senior management and any other representatives and / or the US Audit Committee as deemed appropriate. The US CRO may also engage an independent third party as appropriate to advise on the investigation and resolution of any Significant Concern.

Accountabilities for US-related Whistleblower Concerns

Further to the accountabilities outlined in section 6.0, the following accountabilities apply with respect to handling US-related concerns (i.e. concerns raised in accordance with the Policy that pertain to CUSO):

US Conduct and Culture Risk is responsible for:

- establishing US Region Whistleblower Program procedures for the receipt, retention and treatment of US-related concerns;
- assigning to / collaborating with stakeholders to appropriate groups for investigation, US-related concerns received by US Conduct and Culture Risk in accordance with the Policy, as needed;
- notifying / escalating to appropriate groups as needed in accordance with the Whistleblower Program procedures;
- tracking investigations of US-related concerns and reporting status to Privacy on a quarterly basis;
- reviewing investigation findings / outcomes for US-related concerns with Privacy prior to submission to Privacy for closure (per section 8.2, Privacy is responsible for retention following closure);
- immediately informing Corporate Security of any other concerns that are reported to US Conduct and Culture Risk (i.e. outside of the reporting mechanisms listed in section 3.2) regarding accounting, internal accounting controls or auditing matters;
- informing Privacy of any other concerns reported anonymously to US Conduct and Culture Risk (i.e. outside of the reporting mechanisms listed in section 3.2) that allege misconduct described in section 3.1; **Note:** For the avoidance of doubt, concerns reported to US Conduct and Culture Risk (e.g. Conduct and Culture Risk investigations) are considered not to qualify under the Policy unless they contain an element of a type of misconduct listed in section 3.1);
- reporting to US Audit Committee on a quarterly basis the following:
    - accounting, internal accounting controls or auditing matters reported to Corporate Security from any source or through the Whistleblower Hotline;
    - the status and outcome of all US-related concerns raised under the Policy,
    - the outcome of any root-cause analysis conducted on themes or trends identified among substantiated concerns; and
    - whistleblower concerns regarding the US Operating Committee and Executive Committee members that result in some form of disciplinary outcome beyond coaching.

[8] If a Significant Concern contains an allegation involving the CRO - US Region, US Conduct and Culture Risk will directly notify President & CEO, CIBC Bank USA , SEVP and Group Head, US Region.

US Audit Committee shall:

- provide oversight over, and review on a bi-annual basis, this Policy / Appendix D;
- ensure that procedures have been established for the receipt, retention and treatment of complaints received regarding accounting, internal accounting controls, or auditing matters;
- the confidential, anonymous submission of concerns regarding questionable accounting or auditing matters.
- review and discuss management reports on the procedures and any covered complaints received.

Corporate Security

Corporate Security is responsible for immediately informing US Conduct and Culture Risk of any concerns reported to Corporate Security regarding accounting, internal accounting controls or auditing matters.

Other US Region groups

The following US Region groups shall immediately inform US Conduct and Culture Risk when they receive reports of concerns regarding accounting, internal accounting controls or auditing matters and support US Region investigations as needed:

- US Finance
- US Client Support Center
- US Vendor Risk Management (includes Procurement)
- US Corporate Secretary
- US Human Resources