Sagicor

Wise Financial Thinking for Life

SAGICOR FRAUD & OTHER WRONGDOING POLICY

September 2008

Sagicor Fraud and Other Wrongdoing Policy

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Sagicor, also called the Company, is committed to protecting its revenue, property, proprietary information, corporate reputation and other assets. Sagicor will not tolerate any misuse or misappropriation of its assets or other sharp or unethical business practices. While the Company is committed to the foregoing it is cognizant that great care must be taken to avoid mistaken or false accusations of fraud or other impropriety.

1.2 Sagicor's Fraud and Other Wrongdoing Policy is established to provide guidance and assignment of responsibilities when misuse or misappropriation of Sagicor's assets or other wrongdoing is suspected.

2 SCOPE OF POLICY

2.1 This policy applies to any fraud, suspected fraud, or other wrongdoing, or suspected wrongdoing involving employees, sales representatives, shareholders, directors, consultants, vendors, contractors and / or any other party with a business relationship with Sagicor (applicable person).

2.2 It is Sagicor's intent to investigate any suspected acts of fraud and/or wrongdoing as it is defined in this policy without any regard to the suspected wrongdoer's length of service, position / title, or relationship to the Company. Sagicor reserves the right to take appropriate disciplinary or other action as it deems appropriate.

2.3 This Policy is not designed to question financial and business decisions taken by the Company, nor should it be used to reconsider matters which have already been addressed under other procedures.

3. DEFINITION AND ACTIONS THAT MAY CONSITIUTE FRAUD

3.1 There are many definitions of "fraud"; in its broadest sense fraud is the act of knowingly using deception to secure gain for one's self or another or to cause loss to another. Otherwise stated, fraud refers to any intentional dishonest act committed to secure an unfair or unlawful gain.

3.2 Each individual will be familiar with the types of improprieties that might occur within his or her area of business activity, but for the purpose of guidance, actions constituting fraud may include, but are not limited to:

(i) Forgery or alteration of any document or account belonging to the Company;

(ii) Forgery or alteration of cheque, bank draft, of any other financial document,

(iii) Misappropriation of funds, securities, supplies, or other assets;

(iv) Impropriety in the handing or reporting of money or financial transactions;

(v) Profiteering as a result of insider knowledge of Company activities;

(vi) Disclosing confidential and proprietary information to outside parties;

(vii) Disclosing to other persons securities activities engaged in or contemplated by the Company;

(viii) Any effort to mislead, deceive, manipulate, coerce or inappropriately influence any internal or external accountant or auditor in connection with the preparation, examination, audit or review of any financial statements or records of the Company.

(ix) Misrepresentations or false statements to or by a senior officer or accountant regarding a matter contained in the Company's financial records, financial reports or audit reports.

(x) Legally defined Mail fraud, wire fraud, bank fraud, securities fraud, notation of any role or regulation to fraud against shareholders and/or

(xi) Any similar or related conduct.

4. OTHER INAPPROPRIATE OR WRONGFUL CONDUCT

4.1 There will be instances where the conduct of the applicable person does not rise to the level of fraud as defined by this policy. That conduct however, may nonetheless be considered as inappropriate or improper having regard to its nature, circumstance and generally accepted business practice in the area concerned. Acts of this nature may loosely be called acts of "wrongdoing". Such acts will usually involve improper or questionable moral, ethical, or behavioural conduct on the part of the applicable person and should be reported.

4.2 By way of example, wrongdoing will usually encompasses violations of law, rules, regulations, or codes of business conduct and for the purpose of guidance such wrongful acts include but are not limited to:

(i) Use of company funds or property for any illegal, improper or unethical purpose.

(ii) Tampering with or destroying any Company accounting or audit-related records or documents, except as otherwise permitted or required by Company records retention policy.

(iii) Deliberate error in the preparation, evaluation, review or audit of any of the Company Financial Statements.

(iv) Deliberate error in recording and maintaining Company's financial records.

(v) Deliberate deficiencies in or non-compliance with the Company's internal accounting controls.

(vi) Deviation from full and fair reporting of the Company's financial condition, results of operations or cash flow.

(vii) Accepting or seeking anything of material value from contractors, vendors, or persons providing services / materials to the Company with the exception of gifts less than US$100 in value (for further guidance see also page 11 of Sagicor's Code of Business Conduct and Ethics under the head "Payments, Gifts and Entertainment")

(viii) Destruction, removal or inappropriate use of records, furniture, fixtures, and equipment; and/or

(ix) Any similar or related conduct.

4.3 It is important to note that instances of "fraud" on the one hand and "wrongdoing" on the other may be founded upon the same or similar facts and if there is any question as to whether an action constitutes either fraud or wrongdoing please contact the Legal Department for guidance.

5. RELATED POLICIES

5.1 This is a corporate policy which is designed to supplement other corporate policies such as the Code of Business Conduct and Ethics, the Insider Trading Policy, the Anti Money Laundering Policy, and the Information Technology Security Policy. It is not intended to replace or preclude them. Where there is overlap between the application of this policy and any other policy, the policy most specific to the situation or subject matter will apply.

6. CONFIDENTIALITY

6.1 All participants in a fraud or other investigation shall treat all information received as confidential. Any employee who suspects dishonest or fraudulent activity shall immediately notify the appropriate person as defined in Section 11 – "Reporting Procedures".

6.2 The complainant (otherwise known as the "whistleblower"), should not attempt to personally conduct investigations, interviews or interrogations related to any suspected fraudulent or other act of wrongdoing.

6.3 Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. This is important in order to avoid damaging the reputations of persons suspected but subsequently found innocent of wrongful conduct, and to protect the Company from potential civil liability.

6.4 No information concerning the status of an investigation shall be given out. The proper response to any inquiries is: "*I am not at liberty to discuss this matter*."

6.5 The alleged fraud, wrongdoing or investigation shall not be discussed with the media by any person other than the Vice President, Corporate Communications or designate.

6.6 At no time should an employee, manager or other person report suspected cases of fraud directly to the police. All reports should be made either to the designated senior executives or via the anonymous reporting facility identified in Section 11 – "Reporting Procedures".

7. WHISTLEBLOWER PROTECTION

7.1 This policy is intended to encourage and enable employees and others to raise serious concerns of impropriety regarding the Company's operations within the Company prior to seeking resolution outside the Company.

7.2 No director, officer, employee or other person who in good faith reports a violation or suspected violation of this Policy shall suffer harassment, retaliation or adverse employment consequence. A person covered under this Policy who retaliates against someone who has reported a violation or suspected violation in good faith in accordance with this policy is subject to disciplinary action which may include termination of employment.

8. RESPONSIBILITIES

8.1 Management

8.1.1 Members of management are responsible for establishing and maintaining a system of internal control to ensure the detection and prevention of fraud, waste, abuse and other irregularities within their area of responsibility.

This shall include:

- Being reasonably familiar with the types of fraud or other wrongdoing that might occur within their department;
- Being alert for any indication of fraud or other wrongdoing; and
- Creating and documenting procedures to supplement the Corporate Fraud and Wrongdoing Policy in their respective departments.

8.1.2 Management will support and co-operate with the Legal Department, Internal Audit, the Investigation Unit, other involved departments, and law enforcement agencies in the detection, reporting and investigation of all fraudulent and other wrongful acts, including the prosecution of offenders. Refer to Section 11 – "Reporting Procedures".

8.2 Employees

8.2.1 Any Sagicor employee who knows or has reason to believe that a fraud or other wrongdoing has occurred is responsible for notifying his/her manager. If the employee has reason to believe that the employee's immediate manager may be involved, the employee shall immediately notify a senior manager of the department. Refer to Section 11 – "Reporting Procedures".

8.2.2 It is expected that employees will co-operate fully with management and other involved departments and law enforcement agencies during the course of an investigation and make all reasonable efforts to be available to assist.

8.3. Enterprise Risk Management

8.3.1 Sagicor's enterprise risk management process must systematically assess the various ways that fraud or other wrongdoing can be perpetrated by and against the Company. Risk assessments should also occur when special circumstances arise, such as changes in the operating environment, introduction of new products, entry into new markets and corporate restructuring. This process should identify, evaluate and document the risks of fraud and other wrongdoing.

8.4 Internal Audit

8.4.1 The Internal Audit Department has the primary responsibility for the investigation of all suspected cases of fraudulent or other wrongful conduct as defined in this policy.

8.5 Legal Department

8.5.1 The Legal Department or its designee is the only department/person authorised to provide information to law enforcement or regulatory authorities. All requests for information and/or assistance from such authorities must be immediately forwarded to the Legal Department for determination and handling.

8.5.2 Upon the conclusion of an investigation by the Internal Audit Department, and where further action is being contemplated with respect to an applicable person, the Legal Department or its designee shall become the custodian of all original files (personnel, contractual, etc.) and all individual documents (cancelled cheques, affidavits, etc.) involved in the investigation in order to identify and preserve potential evidence.

8.5.3 Extracts from working papers and files of the investigating team may be released to the Legal Department. However, under no circumstances are these files to be released to any person including law enforcement agents, regulatory authorities and bonding companies, without prior consultation with the Chief Internal Auditor and/or the General Counsel and/or the Chief Executive Officer.

8.6 Audit Committee and Board of Directors

8.6.1 The Audit Committee and the Board of Directors have key oversight roles which must be evidenced in their charters and meeting minutes. They must ensure that management assesses the risks for fraud and other wrongdoing and have controls in place to prevent, deter and detect such activity. They must also ensure that management adheres to stated guidelines for resolving all cases of fraud or other wrongful conduct. A comprehensive review of these policies should be performed at least annually.

8.7 Various Departments

8.7.1 Please refer to Appendix I for the Corporate Fraud and Other Wrongdoing Policy Decision Matrix which assigns primary, secondary and shared responsibilities for actions required with respect to Fraud and other wrongdoing.

8.8 Investigation Unit

8.8.1 The Investigation Unit will usually be an external company, agency or individual who is requested by the Chief Internal Auditor to investigate any report of alleged fraud or other wrongdoing within the Company.

8.9 **Investigation Team**

8.9.1 The Investigating Team are the persons charged with the investigation of an alleged fraud or other wrongdoing and shall include but not be limited to the Chief Internal Auditor, the Investigation Unit and law enforcement agencies.

9. SECURITY OF EVIDENCE

9.1 Once a suspected fraud or other wrongdoing is reported, immediate action to prevent the theft, alteration, and/or destruction of relevant records, both physical and electronic, must occur. Such actions include, but are not necessarily limited to:

(i) Immediately removing the records and placing them in a secure location;

(ii) Limiting access to the location where the records currently exist; and

(iii) Preventing the individuals suspected of committing the fraud or other wrongdoing from having access to the records.

9.2 The records, including mobile devices upon which the same may be stored including mobile telephones, computers, PDAs etc must be adequately secured by the local compliance officer in consultation with the IT and legal departments as appropriate until the Internal Audit Department or Investigation Unit obtains the records to begin the audit investigation.

10. AUTHORIZATION FOR INVESTIGATING SUSPECTED FRAUD OR OTHER WRONGDOING

10.1 The Internal Audit Department, as the department with primary responsibility for the investigation of all suspected fraudulent or other wrongful acts as defined in this policy will, to the extent permissible by applicable domestic law, have:

- Free and unrestricted access to all Company records and premises whether owned or rented.
- The authority to examine, copy, and/or remove all or any portion of the contents of files, desks, cabinets, and other storage facilities on the premises without prior knowledge or consent of any individual who may use or have custody of any such items or facilities when it is within the scope of their investigation.
- The authority to engage the Investigation Unit to lead or assist in an investigation of alleged fraud.

11. REPORTING PROCEDURES

11.1 Great care must be taken in the investigation of suspected cases of fraud or other improprieties so as to avoid mistaken accusations or alerting suspected individuals that an investigation is underway.

11.2 If an individual fails to report a fraud or irregularity, then he or she is in violation of this Policy and is subject to disciplinary action.

11.3 **Employees**

11.3.1 An employee who discovers or suspects fraudulent or other wrongful activity shall contact his or her manager immediately.

11.3.2 If an employee suspects that his or her immediate manager is involved, the employee shall immediate notify the senior manager in the department.

11.3.3 If a CEO, CFO or any Director of the Company is suspected of indulging in fraudulent or other wrongful acts or misstatements, the matter shall be reported to Chief Internal Auditor who shall immediately notify the Group Compliance Officer.

11.4 Managers

11.4.1 Senior Managers and Managers have the same responsibility with respect to reporting fraud and other wrongdoing as do other Sagicor employees and shall report all cases of suspected fraudulent or other impropriety reported to them or within their personal knowledge to the Company Compliance Officer.

11.4.2 If a Manager receives a report of suspected fraud or other wrongdoing from an Employee, the Manager shall instruct the Employee whistleblower not to contact the suspected individual in an effort to determine facts or demand restitution; and, not to discuss the case, facts, suspicions, or allegations with anyone unless specifically asked to do so by the General Counsel, Chief Internal Auditor or the Investigation Unit.

11.5 Company Compliance Officers

11.5.1 Company Compliance Officers who receive reports under this Policy shall forthwith notify the Group Compliance Officer, the Chief Internal Auditor, the local HR department and the Assistant Vice President - Legal and Compliance, Sagicor Financial Corporation.

11.6 Anonymous Reports

11.6.1 As an alternative to the above reporting procedures, any person may report fraud, suspected fraud or other wrongdoing anonymously to Sagicor's Management via phone or the internet. This facility, called "SilentWhistle", is provided by an independent third party company called Allegiance Inc. Anonymous reports can be made 24 hours a day 7 days a week by calling their toll free number **1-888-307-5991** or logging on to http://www.sagicor.silentwhistle.com. Reports made via this facility are forwarded anonymously to Sagicor's management for action. Allegiance Inc. is an organization independent of Sagicor and the identity of the whistleblower cannot be traced by the Company. For further information regarding the use of this facility please refer to Appendix II attached.

11.7 Investigation Inquiries

11.7.1 All inquiries concerning the investigation from the suspected individual, his or her attorney or representative, or any other inquirer should be directed to the General Counsel.

12. TERMINATION

12.1 If an investigation results in a recommendation to terminate an individual, the recommendation will be reviewed for approval by Human Resources, the Legal Department and, if necessary by outside counsel, before any such action is taken.

12.2 The Chief Internal Auditor or the Group Compliance Officer does not have the authority to terminate an employee. The decision to terminate an employee is made by the employee's management. Should the Chief Internal Auditor believe that the management decision is inappropriate having regard to the facts presented; the matter will be escalated to executive level management for a decision.

13. ADMINISTRATION

13.1 The Legal Department is responsible for the administration, revision, interpretation, and application of this policy. The policy will be reviewed annually and revised as needed.

Approved this July 30, 2008.

Chairman
Sagicor Financial Corporation

Appendix I

	Action Required	Investigation Unit	Internal Audit	Finance / Accounting	Executive Management	Line Management	Risk Management	Legal	Communications	Human Resources
1	Controls to Prevent Fraud and other wrongdoing	S	S	S	SR	SR	S	S	S	S
2	Incident Reporting	SR	SR	S	S	S	S	S	S	S
3	Investigations of Fraud and other wrongdoing	SR	SR	-	-	-	-	S	-	S
4	Referrals to Law Enforcement	SR	SR	-	-	-	-	S	-	-
5	Recovery of Monies due to Fraud or other wrongdoing	SR	SR	S	-	-	-	-	-	-
6	Recommendations to Prevent Fraud and other wrongdoing	SR	SR	-	S	S	S	S	S	S
7	Internal Control Reviews	-	P	-	-	-	-	-	-	-
8	Handle Cases of a Sensitive Nature	SR	SR	-	S	-	S	S	-	SR
9	Publicity/Press Release	S	S	-	-	-	-	-	P	-
10	Civil Litigation	S	S	-	-	-	-	P	-	-
11	Corrective Action / Recommendations to Prevent Recurrences	SR	SR	-	S	SR	S	S	-	SR
12	Monitor Recoveries	S	S	P	-	-	-	-	-	-
13	Pro-Active Fraud Training	S	P	-	-	-	-	-	-	-
14	Fraud Education / Training	SR	SR	-	-	S	-	-	S	S
15	Risk Analysis of Areas of Vulnerability	S	S	-	-	-	P	-	-	-
16	Case Analysis	SR	SR	-	-	-	-	-	-	-
17	Hotline		P	-	-	-	-	-	-	-
18	Ethics Line	S	S	-	-	-	-	P	-	-

Legend:
P - Primary Responsibility
S - Secondary Responsibility
SR - Shared Responsibility

APPENDIX II

USING SILENTWHISTLE

Computer:

Step 1: Connect to the Internet from a computer outside of work

Step 2: Type **www.silentwhistle.com** into the address bar and hit "Enter"

Step 3: Search for your company's name

Step 4: Select your company from the list provided. To eliminate the first 4 steps you may go directly to **www.sagicor.silentwhistle.com**

Step 5: Select your method of anonymous communication and enter the desired information.

Note: You need not provide your name or any other form of identifying data.

Telephone:

Step 1: Dial your country's access code selected from the list below.

Step 2: When prompted dial **YOUR TOLL FREE SILENTWHISTLE ACCESS NUMBER 1(888)307-5991** to speak anonymously with a live hotline operator.

Step 3: Provide the operator with the desired information

Access Codes:

Anguilla: 1-800-225-5288

Aruba: 001-800-872-2881

Antigua & Barbuda: 1-800-225-5288

Bahamas: 1-800-872-2881

Barbados: 1-800-225-5288

Belize: 811

Cayman Islands: 1-800-225-5288

Dominica: 1-800-225-5288

Grenada: 1-800-225-5288

Jamaica: 1-800-872-2881

Netherland Antilles (Curaçao and St. Maarten):
001-800-872-2881

Panama: 800-0109

St. Christopher & Nevis: 1-800-225-5288

St. Lucia: 1-800-225-5288

St. Vincent & the Grenadines: 1-800-225-5288

Trinidad & Tobago: 1-800-872-2881

United Kingdom:
0-800-89-0011 (British Telecom)
0-500-89-0011 (C&W)
0-800-013-011 (NTL)

United States: no access code necessary dial toll free number directly.

Online Tutorial

There is an online training module available for SilentWhistle entitled "SilentWhistle: What Every Employee Should Know." This module can be accessed by visiting http://allegiance.webex.com and clicking the "Training Center" tab in the upper left. Once the Training Center page loads, select "Recorded Sessions" from under "Attend a Session" on the left hand side. Click the *play* button on the far right of the module description, fill out the registration information and wait for the class to load. You will be able to pause, stop and rewind the module as necessary.