



CAPITAL ASSURANCE CORPORATION
AND SUBSIDIARIES

ANTI-MONEY LAUNDERING

POLICY AND PROCEDURES

Effective:

May 2, 2006

Updated November 5, 2007

Definitions

Critical Infrastructure Protection

The Office of Critical Infrastructure Protection (“CIP”) and Compliance Policy coordinates the development and implementation of policies regarding: the protection of the critical infrastructure of the financial services sector, including the Department's lead agency role with respect to the financial sector; the development of statutes and regulations within the financial sector, including money laundering, internet gambling and identity theft; and the sharing of information among financial institutions and between the private and public sectors, including financial privacy and the sharing of suspicious information pursuant to the Bank Secrecy Act.

Integration

Integration is the final stage in which an apparently legitimate transaction is used to return the now laundered funds back to the criminal. These stages can occur simultaneously, separately, or overlap.

Layering

Layering is the process of conducting a complex series of financial transactions, with the purpose of hiding the origin of money from criminal activity and hindering any attempt to trace the funds. This stage can consist of multiple securities trades, purchases of financial products such as life insurance or annuities, cash transfers, currency exchanges, or purchases of legitimate businesses.

LIMRA

LIMRA International is a worldwide association providing research, consulting, and other services to nearly 850 insurance and financial services companies in more than 60 countries. LIMRA was established in 1916 to help its member companies maximize their marketing effectiveness.

Definitions (continued)

Money Laundering

Money Laundering is the illegal practice of placing money gained from criminal activity through a series of apparently legitimate transactions in order to hide the criminal origin of the money. The goal is to make money from criminal activity appear to be from legitimate sources. Although money laundering is usually associated with cash, any financial transaction may be a part of a process to hide the origin of the money i.e. non-cash transactions can play a role in money-laundering schemes.

OFAC-Office of Foreign Assets Control

The Office of Foreign Assets Control ("OFAC") of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. OFAC acts under Presidential wartime and national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze foreign assets under U.S. jurisdiction.

Placement

Placement is the initial stage in which money from criminal activities is placed in financial institutions. One of the most common methods of placement is structuring—breaking up currency transactions into portions that fall below the reporting threshold for the specific purpose of avoiding reporting or recordkeeping requirements.

Because most carriers do not accept cash payments, you should be on the look out for cash equivalents.

STATEMENT OF POLICY

Capital Assurance Corporation and its subsidiaries (the “Company”) are strongly committed to preventing the use of its operations for money laundering or any activity, which facilitates money laundering, or the funding of terrorist or criminal activities. Accordingly, the Company will comply with all applicable laws and regulations designed to combat money laundering activity and terrorist financing, including the USA Patriot Act, and will cooperate with the appropriate authorities in efforts to prevent any such misuse of Company products or assets. Every employee is required to act in furtherance of this policy statement the (“AML Policy”) to protect the Company from exploitation by money launderers or terrorists.

As directed by this policy, the Company will:

- Take reasonable steps to determine the true identity of all customers;
- Not knowingly accept funds from or conduct business with customers whose money the Company believes is derived from criminal activity or is intended to conduct, finance or support terrorist activities;
- Not ignore indications that a customer’s money originated from criminal or other money laundering activities or is intended to conduct, finance or support terrorist activities;
- Take appropriate measures, consistent with the law, when the Company becomes aware of facts which lead to a reasonable suspicion of customer activity;
- Cooperate fully with law enforcement and regulatory agencies to the extent that it can do so under all applicable foreign and domestic laws;
- Report all identified instances of suspicious activity to the extent that it can do so under all applicable laws; and
- Comply with all anti-money laundering and anti-terrorism laws and regulations.

All Company employees:

- Are required to read the AML Policy;
- Are required to attend regular AML training programs if their position is designated by this policy as requiring such;
- Should avoid drawing conclusions about customers and their activities based solely on the customer's religious affiliation, ethnicity or national origin; and
- Are prohibited from informing independent agents or customers that their activities have been, may be, or will be reported as suspicious or under investigation.

STATUTORY PROHIBITION AGAINST DISCLOSURE

There are statutory and regulatory prohibitions against the disclosure of information filed in, or the fact of filing, a Suspicious Activity Report ("SAR") whether the report is required or is filed voluntarily. Thus, the Company, its employees and independent agents are specifically prohibited from disclosing that a SAR has been filed (or that the Company has received a copy of filed joint SAR from another financial institution involved in the same transaction) or the information contained therein, except to appropriate law enforcement and regulatory agencies.

If the Company is served with any subpoena requiring disclosure of the fact that a SAR has been filed, or of a copy of the SAR itself, except to the extent that the subpoena is submitted by an appropriate law enforcement or supervisory agency, the Company should neither confirm nor deny the existence of the Suspicious Activity Report. The Company also should immediately notify the Office of Chief Counsel at the Financial Crimes Enforcement Network (703-905-3590).

Any Company employee who violates any applicable AML law or regulation, whether through intentional non-compliance, willful blindness or negligence, is

subject to disciplinary action, such as probation, remedial training, adverse impact on promotions or compensation reviews, or termination. Also, if any Company employee intentionally violates any applicable AML law or regulation, this will be reported to regulatory and law enforcement officials in accordance with local laws and regulations.

DESIGNATION OF COMPLIANCE OFFICER

The persons listed on Appendix A are the designated AML Compliance Officers (“AMLCO”) with overall responsibility for the Company’s Anti-Money Laundering Program (“AML Program”). They are responsible for, among other things:

- Being thoroughly familiar with:
 - the operations of the business itself;
 - all aspects of the Company anti-money laundering program;
 - the requirements of the Bank Secrecy Act;
 - applicable Financial Crimes Enforcement Network forms; and
 - having read carefully all applicable documents issued or posted on the web page of the Financial Crimes Enforcement Network of the United States Department of the Treasury: www.fincen.gov.
- Developing a Risk-Based Program;
- Monitoring of the Company’s compliance with applicable anti-money laundering laws and regulations and with the AML Program and being available to answer all questions posed by employees;
- Updating the AML Program as and when necessary;
- Providing AML training and periodic retraining for employees, independent agents, brokers, and any others doing business with covered products. Designing AML training programs so that these parties have the knowledge necessary to comply with the AML Program; and
- Reviewing all reports from employees of suspicious activity and taking suitable action with respect to such reports.

Any questions regarding this policy or any suspicious questions or actions by customers should be brought promptly to the attention of the AMLCO.

TRAINING

Know Your Customer - Overview

Following Know Your Customer policies and procedures decreases the chance that you or a company will be used to facilitate money-laundering activities. In fact, knowing your customer is the single most important deterrent to money laundering. Not knowingly accepting funds from or conducting business with customers whose money the Company believes is derived from criminal activity or is intended to conduct, finance or support terrorist activities is unacceptable behavior.

Customer Profile

The vast majority of customers are not involved in money laundering, so it is important that you be able to identify routine transactions versus suspicious transactions. Performing a needs analysis for a customer not only helps you meet the Know Your Customer requirements but also benefits our business.

A complete profile for each customer provides you and the Company the ability to:

- Identify appropriate transactions and those that may need heightened scrutiny;
- Detect a pattern of activities that is inconsistent with a customer's stated goals and business;
- Detect inconsistent patterns of transactions;
- Anticipate activities that may or may not be related to money laundering and may require further investigation; and

Also Know Your Customer procedures should include:

- That you make reasonable efforts to:
 - Collect identifying information about the customer,
 - Verify the information, and

- Ensure the financial information that you need to gather for Know Your Customer purposes is information you would normally collect in a needs analysis.

Enhanced Due Diligence

A customer's location, affiliation, or type of business may raise red flags (see additional red flags in Exhibit A) that indicate a need for increased scrutiny.

For example, regulators have identified senior political figures as individuals that require greater due diligence. This enhanced due diligence will be conducted by the Company.

In addition, the following types of customers, entities, and locations have been identified as high risk, and may require enhanced due diligence or additional scrutiny beyond normal due diligence procedures:

- Entities designated by OFAC; and
- Foreign jurisdictions.

Record Retention

Federal rules require that all records mandated under the AML regulations:

- be kept for five years; and
- in a reasonably accessible place and manner.

In addition, all documents related to the opening of accounts and verification of identity as part of a Critical Infrastructure Protection (“CIP”) must be retained for five years after the account is closed and the termination of any policy or contractual agreement with the customer.

If a particular state insurance regulation requires certain documentation to be retained for a longer period, the records must be maintained for the longer time period. Make sure you file any customer identification information you obtain in the customer file along with any information you have provided to the AMLCO.

By documenting your actions, you protect yourself from possible penalties.

As a producer, your responsibility does not end after the initial sale is made. If any of your future interactions with the client seem suspicious, notify the AMLCO. All employees of the Company will be provided a copy of this policy and will be required to read the policy.

In addition to mandatory periodic review of this policy, training will be provided to those employees whose job responsibilities include:

- Direct customer contact;
- Access to view and/or execute customer transactions;
- Processing payments to or from clients or vendors;
- Independent agents actively producing business; and
- Supervisory authority over any employee whose responsibilities are referenced in this section.

This training will take place at the time of implementation of this policy and at least once annually thereafter. All new hires will be provided a copy of this policy as a part of new employee orientation. New hires requiring training will be provided such as a part of new employee orientation. Documentation of employee training will be maintained by the HR department of the Company.

The AML Training Program will consist of a review of these Procedures and any additional programs and materials as the AMLCO officers deem necessary or appropriate from time to time.

Independent Agent Training

All independent agents actively producing business for the Company will be required to complete this Company's training program at the implementation of this policy and annually thereafter. This program will consist of paper or web-based training requiring the independent agent to read the AML Policy and complete a

series of questions to confirm the independent agent's knowledge of the program. The Company's administrative system will maintain a record of the independent agent's compliance with this training program. If the independent agent is in default, no contract provided through this independent agent will be processed until the independent agent fulfills the training requirement under this policy.

The Company has determined that all agents will be required to complete training through our appointed training vendor, LIMRA. Other methods of training will no longer be accepted.

INDEPENDENT AUDIT

There will be a periodic independent audit to test and evaluate compliance with and the effectiveness of the Company's AML Program. The internal audit department of the Company will perform this audit annually.

MONITORING AND REPORTING

Activity Monitoring & Reporting – Suspicious Activities

Suspicious Activity Report (“SAR”)

Employees and independent agents are responsible for identifying the expected activities of your customers in order to establish a range of normal activity. Any activity that falls outside this range should be considered suspicious or unusual. If you suspect or know that a transaction involves funds related to an illegal activity or is designed to avoid regulations, you must report the transaction to the Company's AMLCO.

Through performance of their daily activities, all employees and independent agents shall monitor customer activity. Although no single activity or factor is necessarily

indicative of suspicious activity, all such instances of a single activity or factor that could be indicative, but not necessarily is indicative, of suspicious activity should be reported to the AMLCO. The AMLCO will evaluate such single, potentially suspicious activities together with other factors, such as length of time the Company has known the customer.

All employees and independent agents of the company should frequently review and become familiar with attached Exhibit A, "Suspicious Activity Guidance," that provides an extensive list of potential "red flag" events indicating suspicious activity.

(NOTE: This list should not be considered comprehensive or all-inclusive. Each independent agent or employee must understand the intent of the law so that any suspicious activity – whether listed specifically herein or not – is detected and reported to the AMLCO.)

PROCEDURES

If you identify a suspicious activity, you must not notify the customer. Employees and independent agents are prohibited from informing customers that their activities have been or may be reported as suspicious that a Suspicious Activity Report is filed, or that an ongoing investigation regarding activities in his or her account is being conducted.

In the event that any employee or independent agent becomes aware of any activity listed in Exhibit A attached to this policy, that individual is required to immediately complete the Internal Suspicious Activity Report ("ISAR") (Exhibit B) and submit it to the AMLCO for review.

In the event that any employee or independent agent becomes aware of any activity not listed in Exhibit A but that the individual feels may qualify as suspicious

activity under this policy, that employee or independent agent is required to immediately complete the ISAR and submit it to the AMLCO for review.

Any employee or independent agent receiving an inquiry regarding the AML Policy should immediately report that inquiry to the AMLCO.

The New Business Department will maintain a log of all receipts of Money Orders, Travelers Checks, Certified or Cashier's checks, any other unusual method of payment and federal wire transfers.

AML Compliance Officer will:

- Review and investigate all ISAR submissions;
- Take proper action to dismiss or report the activity to the proper authorities; and
- Review cashier log quarterly for presence of any pattern or suspicious activity; and, Provide AML training and periodic retraining for employees, independent agents, brokers, and any others doing business with covered products.

Company is prohibited from:

- Accepting cash (coin or currency) for any transaction;
- Accepting negotiable checks drawn on independent agent accounts;
- Accepting foreign checks;
- Accepting personal checks drawn on anyone other than the contract owner with the exception of checks drawn on the account of legal guardian of a minor, parent or grandparent of a minor;
 1. At the discretion of the AMLCO, upon further review of a signed statement from the agent and the parties involved detailing the purpose/reason behind the transaction, an

exception may be granted if it can be reasonably determined that the transaction doesn't involve any of the following:

- a. Funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;
 - b. Is designed, whether through structuring or other means, to evade any requirements of any regulation promulgated under the Bank Secrecy Act;
 - c. Has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the Company knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or
 - d. Involves use of the Company to facilitate criminal activity;
- Accepting thirdparty endorsed checks;
 - Issuing checks from any contract to anyone other than that person named on the contract (except in the case of death); and
 - Issuing any contract sold by an independent agent who has not completed the AML Training Program.

Civil and Criminal Penalties

The penalties associated with money laundering are severe.

- Fines may be twice the amount of the transaction up to \$1 million.
- Property involved in the transaction may also be subject to seizure and forfeiture.
- Employees of financial institutions can be fined individually and sentenced to up to 20 years of imprisonment for knowing or being willfully blind to the fact that the transaction involved illegal funds.

You can protect yourself from charges of willful blindness by reporting any suspicious behavior to the AMLCO and keeping documentation of your report.

APPENDIX A
Designation of Compliance Officer

Anti Money Laundering Compliance Officers:
(Effective October 23, 2007)

PRIMARY CONTACT

Stephen M. Coons
Chief Compliance Officer
317-574-2661

Charles Storm
Administration Director
317-574-4064

Gerald (Jerry) Hochgesang
Director of Financial Transactions
10689 N. Pennsylvania Street Indianapolis IN 46280
317-574-6230

EXHIBIT A: Suspicious Activity Guidance

Examples of suspicious activities (“red flags”) with regard to insurance products include but are not limited to:

- The customer exhibits unusual concern regarding the firm's compliance with government reporting requirements and the firm's AML policies, particularly with respect to his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspect identification or business documents.
- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business strategy.
- Application for a policy from a potential customer in a foreign location where a comparable policy could be provided "closer to home."
- Introduction by an agent intermediary in an unregulated or loosely regulated jurisdiction or where organized criminal activities (e.g., drug trafficking or terrorism) are prevalent.
- Applicant for insurance business uses a mailing address outside of the insurance regulator's jurisdiction and where the home telephone has been disconnected, upon verification attempt.
- Requests for a large purchase of a lump sum contract where the customer's experience is small, regular payments contracts, unless there are appropriate reasons.
- Applicant for insurance business requests to make a lump-sum payment by a wire transfer or with foreign currency.
- Transfers of the benefit of a product to an apparently unrelated third party.
- Changes of address or changes of customers to foreign countries.
- Attempts to use a third-party check to make a proposed purchase of a policy.
- Applicants with no concern for the performance of the policy but much concern for the early cancellation.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.

EXHIBIT A: Suspicious Activity Guidance (continued)

- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
- The customer exhibits a lack of concern regarding risks, commissions, surrender charges or other transaction costs.
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the firm's policies relating to the deposit of cash and cash equivalents.
- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the \$10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third party transfers.
- The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the Financial Action Task Force.
- The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.
- The customer's account shows numerous currency or cashiers check transactions aggregating to significant sums.
- The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.

EXHIBIT A: Suspicious Activity Guidance (continued)

- The customer's account has wire transfers that have no apparent business purpose to or from a country identified as money laundering risk or a bank secrecy haven.
- The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
- The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
- The customer requests that a transaction be processed in such a manner to avoid the firm's normal documentation requirements.
- The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as penny stocks, Regulation S ("Reg S") stocks, and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)
- The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.
- Attempt to borrow maximum cash value of a single premium policy soon after purchase.