ANTI-MONEY LAUNDERING COMPLIANCE POLICY

Summary

IAG ("the Company") upholds the highest professional standards in confidentiality and compliance when managing client and third-party information and business best practices. We also ensure that the Insurers with which we place business are compliant through every step of the policy placement and management process.

This policy applies to all colleagues of IAG. IAG is committed to meeting our responsibilities to prevent and detect money laundering and terrorist financing. These responsibilities generally include complying with all applicable anti-money laundering laws and regulations, including risk-based customer due diligence and reporting suspicious activity consistent with applicable laws.

The geographies in which IAG conducts business have laws against money laundering, which prohibit financial transactions involving the proceeds of criminal activities. Failing to detect and prevent these kinds of transactions, or to comply with applicable laws and regulations that are intended to prevent and detect money laundering, could subject the Company and/or the individuals involved to civil and criminal penalties and could severely damage the Company's reputation. This policy requires that IAG enforces a set of protocols to any risk-based anti-money laundering activities detected among our clients to mitigate risks to our firm.

Defining Money Laundering

Money laundering is any process used to conceal the true origin or ownership of the proceeds of criminal activities. The aim of a money laundering operation is to make the illegally obtained or used money difficult to trace and to appear as if it is derived from a legitimate source. Consequently, many money laundering operations can be deliberately complex.

Money laundering generally encompasses any type of financial transaction which involved the proceeds of an illegal act, including fraud, embezzlement, drug trafficking, or public corruption. Money laundering can also involve the use of legitimate funds to facilitate criminal activity, such as terrorist financing, and can be implicated in tax evasion schemes. Money laundering is not limited to cash transactions. It can involve wire transfers, cheques and financial products, including insurance policies and investment portfolios.

What Qualifies as Suspicious Activity

A suspicious activity can be related to any type of business relationship and include the following scenarios:

- The individual or entity has difficulty describing the nature of their business or lacks general knowledge of their industry practices;

- The individual or entity has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations or unethical conduct;

- Funds are sent by wire transfer without usual originator information or from a bank account that is not in the client's name or from a financial institution that is not geographically logical for the client;

- Payments are made with money orders, traveler's cheques, cashier's cheques or bank drafts;
- Overpayments or duplicate payments are made and it is requested that the refund of the excess payment be made to a third party or to an account at a financial institution that is not geographically logical for the client;
- Payments are made from a client's personal account instead of a business account;
- Payments are made by a third party without a logical relationship to the client;
- Multiple instruments are received to make a single payment (i.e. multiple cheques and/or wire transfers to pay a single invoice);
- The client wishes to engage in transactions that lack business sense or are inconsistent with the client's stated business strategy;
- The information provided regarding the source of funds is false, misleading or substantially incorrect; or
- The client has requested invoicing accommodations that do not fit the normal business standards for services provided.

Suspicious activities related to insurance business transactions include:

- The applicant for insurance attempts to use cash to complete a proposed transaction when this type of business transaction would normally be handled by cheques;
- The applicant for insurance shows no concern for the performance of the policy, but much interest in the early cancellation of the contract;
- The product is terminated early for no apparently legitimate commercial reason or purpose, especially at a loss in which cash was tendered and/or the refund check is to a third party;
- A transfer of the benefit of a product is made to a third party that has no apparently legitimate connection to the policyholder or insurance transaction; or
- The designated beneficiary for an individual life insurance policy (at inception or through changes) does not appear to have a logical relationship to the policy owner.

COLLEAGUE RESPONSIBILITIES

Understanding Client Operations

IAG colleagues must be alert to any information or suggestion that a client could be engaging in money laundering or other illicit activities, or could be owned by or do business with individuals or entities that engage in illicit activities. Any of the circumstances listed above as suspicious activity, as well as any evidence a client could be associated with corrupt individuals or criminal elements or appears on an applicable government sanctions list should be immediately reported to the compliance officer.

The most critical defense against money laundering is for IAG colleagues to understand their client's operations. IAG will establish procedures in accordance with local laws and regulations for monitoring and/or investigating client activities. It is every IAG colleague's responsibility to follow procedures set for by the Company, including:

- Determining and verifying the true identity of the client or prospect based on documents, data or information obtained from a reliable and independent source before establishing a business relationship;

- Taking reasonable care to know, with an appropriate degree of confidence, the type of business and transactions the client or prospect is likely to undertake and the client's sources of funds;

- Obtaining information about the client or entity's underlying beneficial owners, depending on the risk presented by the client or prospect;

- Notifying and consulting with IAG's compliance officer before proceeding with a business or financial transaction if the findings from a due diligence review rise to anti-money laundering concerns or if the colleague becomes aware at any time of transactions that are not consistent with the client's normal business activities;

- Updating client information and due diligence procedures on a periodic basis depending on the money laundering or terrorist financing risk of the client, or more frequently if there are significant changes in the client's business ownership, activities or other relevant information that raises concerns.

Forms of Payment

If an IAG colleague is involved with receiving or handling funds, they are required to:

- Follow compliance procedures for cash transactions, duplicate or overpayments, unallocated receipts, acceptable forms of payment, payments from parties unrelated to the client and payment requests to a third party not associated with the underlying transaction. Cash, money orders, cashier's cheques, bank drafts, gift cards, traveler's cheques, courtesy tickets and payments from third parties unrelated to the client are not accepted without risk-mitigating controls approved by IAG's directors. Examples of acceptable forms of payment include a check drawn on an account in the client's name or a wire

transfer that identifies the client as the originator or ordering party. Payment should be made with a single check or wire transfer in the full amount due from an account with a financial institution in a geographic location that is logical for the client; and

- Be vigilant when any payment request or proposed flow of funds appears unusual.

An IAG colleague is required to contact the IAG compliance officer immediately for guidance if:

- A client attempts to make a payment by multiple means to pay a single invoice (i.e. multiple cheques, money orders, cashier's cheques, money orders, traveler's cheques and/or wire transfers);
- Payments are received from third parties unrelated to the client;
- A client has, on a recurring basis, significantly overpaid the amounts due from them, or paid duplicate amounts for the same invoice;
- A client makes a payment significantly greater than the invoice amount and/or a duplicate payment and requests to refund the excess payment to a third party not otherwise directly involved in the transaction; or
- A payment is unusual or suspicious.

Suspicious Activity Reporting

Unusual or suspicious activity can occur at any stage during a business relationship. To deem a client's activity as suspicious, IAG colleagues must:

- Be familiar with the signs that could indicate money laundering and be alert to any signs of suspicious activity, as noted above;
- Notify and consult with IAG's management if, at any time during the client relationship, a colleague observes any suspicious activities that may indicate money laundering or otherwise inappropriate business transactions;
- Under no circumstances is an IAG colleague required or advised to contact the entity in question regarding suspected money laundering or inappropriate business transactions or proceed with the transaction without prior approval from a IAG management. Contacting the entity in question regarding questionable or suspicious activity, often referred to as "tipping off", may be a criminal offense in some countries; and
- Be aware and comply with applicable laws governing the reporting of suspicious activity and comply with relevant privacy laws which may limit or affect the kinds of information that can be shared about clients or suspicious activities.

MANAGEMENT RESPONSIBILITIES

IAG managers must follow and implement the Company's risk-based compliance procedures, including:

- Communicate and escalate issues relating to anti-money laundering to IAG's President and abide by local laws regarding anti-money laundering reporting;
- Annually and periodically, as required, perform a risk assessment of all clients under management to identify each business' degree of risk and report findings, including advisable changes to IAG's anti-money laundering policy. Any new products or services offered to a client must be evaluated by IAG managers for the degree of anti-money laundering risk before implementation;
- Inform new and existing clients of IAG's anti-money laundering procedures based on the client's business risk and the legal reporting requirements in the client's jurisdiction of operation;
- Provide initial and periodic training and awareness communications to IAG colleagues;
- Monitor unacceptable forms of payments to the extent feasible and establish appropriate controls on cash transactions, duplicate or overpayment amounts unallocated receipts, acceptable payment methods and payment requests to third parties not associated with the underlying transaction; and
- Follow all applicable government cash and other transaction reporting and recordkeeping requirements.

Documentation

Where procedures require due diligence, IAG colleagues are required to:

- Retain all identifying information provided by the client, as well as the methods and results of the verification;
- Satisfy, within a reasonable amount of time, any inquiry for such documentation from an IAG internal audit, legal advisors or governmental regulatory authorities and law enforcement agencies; and
- Retain all key anti-money laundering-related documents and files in original or electronic format for a minimum of five years from the date that a client relationship is terminated, a transaction is conducted or a suspicious activity report is filed consistent with local regulations or longer if required by other record retention policies.

Training and Compliance

This policy applies to all colleagues of IAG and training in the protocols of this policy will be required by all new and existing employees. Failure to comply with this policy may result in disciplinary action in accordance

with local laws and internal procedures, including termination of employment or contract for services. Failure to comply with applicable anti-money laundering laws and regulations may also subject employees to criminal prosecution and penalties.

Transparency and Auditing

Internal audits will be conducted on an annual basis and periodically as required. All audit findings will be reported to IAG management, as appropriate.

For more information about our privacy policies and procedures, please contact our Compliance Officers:

Guy Bentley, President
Telephone: (416) 363-0072
Fax: (416) 363-0060
Email: gbentley@iagi.ca

Lori Bentley, Operations Manager
Telephone: (416) 363-0075
Fax: (416) 363-0060
Email: lbentley@iagi.ca