IGC
JEWELRY & DIAMONDS
| THE MAKE MATTERS |

67 E Madison #1816
Chicago, IL 60603
United States

T 800-344-6605
F 312-372-3924

concierge@igcjd.com
www.igcjd.com

ANTI-MONEY LAUNDERING

GROUP POLICIES & PROCEDURES

Anti-Money Laundering, Anti-Terrorism Financing, and Other Financial Crimes

IGCJD's AML Policies and Procedures are based on the IGC GROUP Policies and Procedures, with whom IGCJD cooperates for all compliance matters. In these AML Group Policies and Procedures, IGCJD is considered a Member Entity of IGC Group.

Dr. Anne-Marie De Scheemaecker
November 2017/Update July 2024

A. De Scheemaecker

Table of Contents 1

1. Corporate Integrity

IGC Group of Companies (IGC) is committed to conduct its operations with honesty, integrity, openness; with respect for the human rights and interests of its employees and their communities; with respect for the environment; and in adherence to the highest ethical standards. IGC complies with the diamond industry's Best Practice Principles (BPP) through its De Beers Global Sightholder Sales (DBGSS) affiliation as well as the jewelry industry's Code of Practices (COP) through the Certified Membership of the Responsible Jewelry Council (RJC).

The Group Compliance Officer, assisted by the local Compliance Officers at the IGC Member Entities around the world, is committed to monitor IGC's compliance with the BPP, COP, and all national and applicable international rules and regulations addressing money laundering and other financial crimes.

IGC honors the legitimate interests of all its business partners and is committed to contending dishonesty and fraud in all its transactions so to maintain and enhance consumer trust in, and the reputation of, the diamond and diamond jewelry industries. No practice or conduct will be undertaken nor allowed by any of IGC's managers and employees globally that could bring the diamond or diamond jewelry industry into disrepute. All IGC Member Entities are required to comply with the laws and regulations of the countries in which they operate.

2. Business Partners

IGC is dedicated to establish mutually beneficial relations with its customers, suppliers, and other business partners throughout its global supply chain, and expects its business partners to adhere to business principles that are consistent with theirs. Therefore, IGC will use *Best Endeavors* to ensure the commitment of its diamond suppliers, its diamond customers, and if applicable, its subcontractors to comply with the BPP and COP. IGC is conducting strict and ongoing due diligence on the business relationships and scrutinizes

all transactions undertaken throughout the course of that relationship to ensure that the transactions are consistent with IGC's identification and knowledge of the customers, suppliers, and business partners, as well as their business and risk profile, including the source of funds if deemed necessary.

3. Trade-Based Money Laundering

Following the high value of diamonds and the easiness of their transportation, the diamond sector is particularly vulnerable to money laundering in the form of disguising proceeds of crimes by moving the value through trade transactions and as such legitimizing the illicit origin.

4. Anti-Money Laundering and Anti-Financial Crime Statement

All Member Entities of the IGC are committed to the highest standards of Anti-Money Laundering (AML) and Anti-Financial Crime (AFC), including but not limited to, Anti-Bribery and Corruption (ABC), Counter-Terrorism Financing (CTF), Anti-Fraud, and other indictable financial crimes, such as smuggling, embezzlement, racketeering, transfer pricing, illegal trade, and tax evasion.

IGC will only conduct business with companies whose business is legal and whose funds come from legitimate sources. Money laundering is facilitated through the use of shell companies, structuring deposits, smurfing, overseas banking, and/or underground banking, and therefore, such means are intensively triggered and investigated.

IGC has its headquarters in Antwerp, Belgium, and is supervised by the Belgian Federal Financial Supervisory Authority under the Royal Decree dd. 7 October 2013 regarding AML/AFC for the diamond industry. Belgium is a member country of the Financial Action Task Force (FATF) and the European Union (EU).

IGC has enacted laws and rules at each IGC Member Entity designed to implement the anti-money laundering policies of global organizations contending money laundering and terrorist financing, including FATF, the U.S. Patriot Act, the Bank Secrecy Act (BSA), and the EU Anti-Money Laundering Directive. The purpose of these laws is to detect, prevent, and report any issue regarding potential money laundering, fraud, terrorist financing, bribery, facilitation, or other financial crimes. IGC Member Entities globally are subject to the same strict due diligence and comprehensive measures.

Additionally, as a De Beers Sightholder and RJC Certified Member, IGC is compelled to comply with AML, ABC, CTF, and other AFC regulations stipulated in the respective BPPs and COPs. IGC strictly adheres to all applicable laws and regulations in all the countries where it conducts business or has a business relationships to. IGC examines its AML and AFC strategies, purposes, and objectives on an ongoing basis and maintains an effective program for the Group's business that reflects those best practices and principles.

5. Governance Framework

The Group Compliance Officer (GCO) has been assigned by the Board of Directors (BOD) with a Group-wide discretionary power over AML and AFC-related matters. The GCO has unrestricted access to all information, data, records, and systems at all IGC Member Entities considered necessary to fulfill his/her obligations, and reports directly to the BOD.

The GCO is responsible for Group-wide adherence to applicable AML and AFC regulations and obligations as well as for establishing and maintaining IGC's AML/AFC program to identify, assess, monitor, and manage risks related to money laundering, terrorist financing, and other financial crimes. At each Member Entity of IGC Group, a local Compliance Officer is appointed who is responsible for the Member Entity's adherence to applicable AML and AFC regulations and obligations. Any potential issue or suspicion must be reported to the GCO immediately, who will further assist in investigating the issue and deciding whether reporting to the respective AML Authorities is required.

6. Policies and Procedures

IGC has developed a clear set of policies and procedures outlining its general AML/AFC standards and principles. Detailed documents and forms are used to ensure that these standards are implemented into day-to-day business practices at each IGC Member Entity worldwide.

All policies and procedures are published in a public folder on the IGC Member's local server, which enables managers and employees to consult them at any time. The policies and procedures are subject to an annual review and are updated if applicable to ensure conformity with current AML/AFC laws and regulations.

6.1. Bribery and Facilitating Payments

Each IGC Member Entity will conduct its operations in accordance with the principles of fair competition and all applicable laws and regulations.

Managers and employees may not offer or accept any gift which is, or can be considered as, being a bribe or facilitating payment. The accounting records of the IGC Member Entity and the supporting documents must accurately describe and reflect the nature of the underlying transactions, and are subject to regular and independent review.

IGC prohibits bribery in all its business practices carried out on its behalf by its managers, employees, agents, and/or business partners. It is prohibited

- to offer, accept, or condone any payments, gifts in kind, hospitality expenses or promises as such, that may compromise the principles of fair competition or constitute an attempt to obtain or retain business
- to direct business to any person or company to influence the course of any business or governmental decision-making process.

For each Member Entity, IGC requires its managers and employees to report any attempted bribery or facilitating payment to their Compliance Officer, who will immediately inform the Group Compliance Officer. Managers and employees will not suffer any adverse consequences or penalties for voicing concerns or reporting attempts of bribery or facilitating payment to the company, its corporate head office, or the authorities.

IGC requires to communicate its Anti-Bribery Policy to all new managers, employees, customers, suppliers, and business partners. Suppliers must submit detailed invoices for goods and services purchased by the company before the payment of the invoice is approved. Only invoices that correspond with the delivered goods and services, including the correct amounts and correct prices, will be approved for payment by wire or by cheque.

IGC prohibits hiring managers and employees or entering into a business relationship with new customers, suppliers, and business partners without the completion of a comprehensive internal risk assessment. IGC prohibits entering or retaining a business relationship with any managers, employees, customers,

suppliers, agents, or other business partners who are believed to pose a risk for bribery or facilitating payment.

6.2. Anti-Money Laundering, Terrorism Financing, and Financial Crimes

IGC will, at all times, comply with national and relevant international laws and legislations regarding money laundering, terrorism financing, and other financial offences.

IGC has implemented a strict Group-wide KYC program to ensure all customers, suppliers, and other business partners are subject to adequate identification, risk rating, and monitoring measures. The program has been implemented globally at all IGC Member Entities and data are centralized and accessible in the Group's secured CRM platform.

6.2.1. Identification and Verification: Know Your Customer (KYC)

- All IGC Member Entities will identify and verify the identity of all their customers, suppliers, and business partners using reliable, independent source documents, data, and information.
- All customers, suppliers, and business partners are required to provide proof of incorporation or similar evidence of the legal status of the legal person or arrangement, as well as information concerning the business partner's name, the names of trustees, legal form, address, directors, and provisions regulating the power to bind the legal person or arrangement.
- Any person purporting to act on behalf of the customer, supplier, or other business partner must validate that he/she is authorized to do so, and the identity of the person must be provided.
- All new customers and suppliers must complete the Customer/Supplier Verification Form.
- Each IGC Member Entity must take reasonable measures to identify and verify the identity of the Ultimate Beneficial Owner (UBO) of any customer, supplier, or other business partner, including forming an understanding of the

ownership and control structure, such that the IGC Member Entity is satisfied that it knows who the UBO is. The type of measures needed to satisfactorily perform this function would require the following actions:

- identification of the UBOs: the natural persons who, whether acting alone or together or through one or more juridical persons, exercise control through ownership or voting rights, or who ultimately have a controlling ownership interest.
- if unable to identify the UBO, identification of the natural persons who comprise the Senior Management of the legal person or arrangement.
- after identification of the UBO or Senior Management: verification of the data through the *Bureau Van Dijk* global KYC Database, which contains 250 million companies worldwide with information about directors, shareholders, UBOs, FATF countries, sanction lists, and individuals worldwide, and to which IGC has access. The database comprises two sets of data:
  - *Orbis*: Company Verification Database
  - *WorldCompliance*: Individuals Verification Database

- Where the customer, supplier, or the owner of the controlling interest is a *public listed company* that is subject to regulatory disclosure requirements, it is not necessary to seek identification and verification of the identity of any shareholder of that company.
- Depending on the location of the IGC Member Entity, following additional documentation is required:
  - AML declaration completed and signed;
  - BPP/RJC declaration completed and signed;
  - U.S. Patriot Act and BSA Compliance Form completed and signed.

The IGC Member Entity must conduct ongoing due diligence on their business relationships and scrutinize all transactions undertaken throughout the course of that relationship. Any customer, supplier, or other business partner with whom no transactions have been conducted over the past 12 months, and with whom a new

transaction is presented, will automatically be subject to a fresh and integral KYC identification and verification procedure.

IGC bears the ultimate responsibility for accepting a business partner and conducting a transaction. Therefore, strict and comprehensive due diligence is substantial to protect IGC and its business.

6.2.2. Risk Assessment, Management, and Mitigation

Each Member Entity must identify, assess, and prioritize potential risk and undertake the required actions to mitigate, monitor, minimize, and control the probability of money laundering activity. The Compliance Officer at each IGC Member Entity must intensify his/her investigation measures to the degree of perceived risk in situations that seem to bear an increased chance of money laundering or terrorism financing.

6.2.3. AML/AFC Risk Analysis

IGC has implemented an ongoing AML/AFC Risk Analysis process to assess the level of risk exposure presented in the view of the Group's customers, suppliers, business partners, and/or their geographical location/country, and to develop appropriate security measures from this analysis. AML safeguards are derived from the results of the AML Risk Analysis. Based on objective risk criteria, customers, suppliers, and business partners are divided into categories depending on the perceived level of risk:

Limited Risk

A limited risk is considered when:

- it is unclear what kind of business relationship the customer, supplier, or business partner wants to engage in;
- the purpose and motive for the business transaction are questionable;

- the customer, supplier, or business partner is unable to provide any clarification for the intended transaction;
- the customer, supplier, or business partner asks unusual questions or requires peculiar sets of conditions.

Higher Risk

A higher risk is considered when:

- no face-to-face meeting takes place at the identification and transaction: i.e. the customer is not physically present for identification. For example online sales via a platform and sales by phone;
- the transaction is done with or on behalf of political prominent persons (PPPs) or politically exposed persons (PEPs), who have or have held prominent political positions, or with their direct family members and/or close associates;
- the customer, supplier, or business partner
    - is based in a high risk third country that is black-listed by the FATF (see country risk);
    - is active in sectors other than diamond and diamond jewelry;
    - suggests an atypical payment method;
    - frequently changes bank accounts or business trading partners without a plausible explanation;
    - is new and/or has little experience in the diamond or diamond jewelry sector;
    - has a questionable structure and/or arrangement of ownership.

Unacceptable Risk

An unacceptable risk is considered when:

- a bad experience with the customer, supplier, or business partner has happened in the past;
- false or forged information has been provided in the past;
- the customer, supplier, or business partner
    - asks to refrain from carrying out an investigation in return for money;
    - is on a terrorist or fugitive suspects list;
    - is on a sanctions or embargo list;
    - was convicted for a serious crime;
    - insists on a transaction in cash.

Country-Risk

The following countries have been identified by FATF and EU (5th AML Directive) as bearing high AML risk (retrieved from http://www.fatf-gafi.org/countries/#high-risk): [June 2024]

A. High risk call for action:

- Democratic People's Republic of Korea (DPKR)
- Iran
- Myanmar

B. High risk under increased monitoring:

- Bulgaria
- Burkina Faso
- Cameroon
- Croatia
- Democratic Republic of Congo
- Haiti
- Kenia
- Mali
- Monaco
- Mozambique

- Nigeria
- Mozambique
- Namibia
- Nigeria
- Philippines
- Senegal
- South Africa
- South Sudan
- Syria
- Tanzania
- Venezuela
- Vietnam
- Yemen
- Zimbabwe

6.2.3.1. Management and Control

The IGC AML/AFC program is formulated and globally directed by the Group Compliance Officer and addresses all AML/AFC-related topics, in particular KYC, ABC, and Anti-Fraud. For all these topics, IGC has developed and implemented a comprehensive set of measures to identify, manage, and control potential risks, which must be complied with globally by all IGC Member Entity managers and employees. The IGC internal organization enables each Member Entity to centralize and communicate information to detect, mitigate, and inhibit transactions related to money laundering, terrorism financing, and other financial crimes.

In each IGC Member Entity, the Compliance Officer must ensure compliance within his/her Entity with the following obligations:

- ensure that the Entity complies with obligations drafted under the Anti-Money Laundering policy
- ensure that the Entity complies with the applicable *cash limitations* (see Appendix A)
- ensure to provide a written or electronic Annual Activity Report

- act as a *bonus pater familias.*

6.2.3.2. Customer Acceptance Policy (CAP)

Each IGC Member Entity applies a customer/supplier/business partner acceptance policy, allowing to investigate in advance the risk of money laundering or terrorist financing associated with the profile of the client and with the nature of the business relationship or the desired transaction. No transaction can take place without the prior formal approval by the local Compliance Officer, the GCO, or a member of the IGC Member Entity's BOD.

The General Principles of the CAP are the following:

- the Member Entity must classify customers, supplier, and business partners into the various risk categories as described in §6.2.2.1., and decide on the acceptance criteria for each category based on the risk perception.
- where the customer, supplier, or business partner is a prospect, the account will be opened only after the relevant due diligence and identification measures and procedures have been conducted, the Customer/Supplier Verification Form has been completed, the required documentation and signed documents have been collected, and the account has been approved by the Compliance Officer, the GCO, or the BOD.

6.2.3.3. Prohibited Business Relationships

The IGC Member Entity must refuse any business transaction or enter into a business relationship if the Member Entity is not convinced that it knows the true identity of the business partner, its UBO, and/or the nature of the business; or if the formal requirements concerning the identification of the customer/supplier and/or its UBOs are not met. Each Member Entity must intensify its investigation measures to the degree of perceived risk as described in §6.2.2.1.

Furthermore, the IGC Member Entity will not

- conduct any business transaction with customers/suppliers who are perceived as bearing an increased risk of money laundering or terrorism financing;

- accept payments that are known or suspected to be the proceeds of criminal activity
- enter into/maintain business relationships with individuals or entities known or suspected to be a terrorist or a criminal organization, or member of such, or listed on sanction lists
- enter into a business relationship with customers/suppliers from High Risk Countries
- enter into a business relationship with customers/suppliers who refuse to disclose their identity, UBOs, and/or company registration forms
- enter into/maintain a business relationship with customers/suppliers who insist in paying by cash
- open any account in anonymous or fictitious names.

6.2.3.4. Group-Wide Controls

Adherence to the Group-wide AML/AFC program is audited by the GCO on a regular basis (minimum once per year) for each IGC Member Entity, to ensure that IGC's efforts are successful. The local Compliance Officers at each Member Entity are therefore obliged to implement and conduct appropriate customer and supplier-related controls in order to ensure that all applicable AML and AFC requirements are being adhered to and that security measures are properly functioning. The GCO further ensures that controls are comparable and equally comprehensive across all IGC Member Entities.

6.2.3.5. Embargo Regulations

IGC ensures to comply with all embargo regulations globally as required through the Bank Secrecy Act. IGC is considering the potential risks in designing, implementing and testing its anti-money laundering and trade embargo compliance program.

6.2.4. Filing of Suspicious Activity and Transaction Reports (SARs)

Suspicious activities and/or transactions must be properly handled and intensified within the respective IGC Member Entities. This is the case when:

- the business has received or is about to receive the proceeds of unlawful activities;
- a transaction or series of transactions will take place to which the business is a party, facilitated, or is likely to facilitate the transfer of unlawful activities;
- the transaction has no apparent business or lawful purpose;
- the transaction is conducted for the purpose of avoiding giving rise to a reporting duty under AML laws and regulations;
- the transaction may be relevant to the investigation of an evasion or attempted evasion of a duty to pay any tax, duty, or levy imposed by the country;
- the business has been or is about to be used for money laundering purposes;

Such must be immediately reported to the Compliance Officer and GCO, whereas:

- the Compliance Officer and/or GCO must examine such reports,
- the Compliance Officer communicates with the GCO regarding the reporting of suspicious activities
- the Compliance Officer must ensure the flow of information to the relevant Financial Intelligence Processing Unit (FIU) or Anti-Money Laundering Authority (AMLA) in the form of special reporting before the transaction is carried out (see Appendix B).
- Exception: Notification may take place immediately after the execution of the transaction, provided that:
  - it is not possible to postpone the execution of the transaction in view of its nature;
  - such postponement could obstruct prosecution of the beneficiaries of the alleged money laundering or financing of terrorism
- in the event that an employee discovers an unusual or suspicious transaction which involves a member(s) of the Management of the IGC Member Entity, the employee must then immediately report the transaction to the GCO and/or the Member Entity BOD.
- in the event of any amendment to legislation or regulation, where required, any relevant obligation or protocol required of the IGC Member Entity must be adopted as policy and practical effect will be given thereto in the form of

the introduction of appropriate procedures, including but not limited to the reporting of cash transactions above the threshold (see Appendix A).

6.2.5. Training and Awareness Program

The diamond sector federation Antwerp World Diamond Center (AWDC) regularly organizes seminars for directors and compliance officers of Belgian registered diamond trading companies, where up-to-date guidelines and information are shared and explained. These seminars are attended on a regular basis by the responsible executives and officers of IGC Group in Antwerp.

Across the Group, IGC has implemented an AML/AFC education and training program to ensure that all relevant managers and employees undergo a comprehensive awareness and sensitizing education and training. This training program is based on the guidance received from AWDC and tailored to the diamond and diamond jewelry business, so to ensure that managers and employees are aware of the various potential patterns and techniques of money laundering and financial crime that may occur in their daily business operations.

Training covers the general obligations arising from applicable, legal, and regulatory requirements as well as internal policies, procedures, and communication means. It further includes the resulting discrete duties which must be adhered to in everyday business as well as typologies to recognize money laundering or financial crime activities and transactions.

Regular AML training at each IGC Member Entity globally is provided by the GCO to ensure that all relevant managers and employees are reminded of their duty to timely report any suspicious activity to their respective local Compliance Officers and next to the GCO. In case it would occur, the necessary steps will then be taken to file and report unusual or suspicious activities and transactions.

Finally, the training incorporates the identification and reporting of transactions that must be reported to the local Financial Intelligence Unit (FIU) for each IGC Member Entity.

6.2.5.1. Reliability and Obligations of Managers and Employees

IGC Group applies hiring policies that help ensuring that only reliable managers and employees are employed. Each IGC Member Entity appoints one Compliance Officer who has the professional experience, the due diligence, the hierarchical level, and the authority needed to exercise his/her function.

Managers and employees will be liable for the failure to report information or suspicion regarding money laundering or terrorist financing to the Compliance Officer. Managers and employees must cooperate and report, without delay, anything that comes to their attention in relation to transactions for which there is a slight suspicion that they are related to money laundering or terrorist financing.

6.2.6. Audits

Both internal and external third-party audits are organized on a regular basis at each of the IGC Member Entities to verify compliance with the AML/AFC laws and regulations.

6.2.6.1. Internal AML Audit

The Group Compliance Officer (GCO) will perform an internal audit at least once per year at each of the IGC Member Entities to review and evaluate the appropriateness, effectiveness, and adequacy of the policy, practices, measures, procedures, and control mechanisms applied for the prevention of money laundering and terrorist financing. The local Compliance Officer will perform an internal audit at a regular basis to verify compliance with the AML/AFC requirements. The internal audit comprises of:

- a random sample of sales and purchase invoices from the previous calendar year, including at least five domestic and, if applicable, five international transactions;
- verification of the payment records and bank statements of the paid invoices for conformity with AML/AFC requirements;
- verification of the customer/supplier KYC records, based on the IGC Member Entity local requirements, laws, and regulations;
- in the case of nonconformance or remarks, a full review of all accounts id performed;

- provision of internal audit report

6.2.6.2. External AML/AFC Audit

As a De Beers Sightholder, IGC is required to adhere to De Beers' BPPs, including AML/AFC practices. Through an independent and internationally qualified auditor (SGS), De Beers performs:

- annual desktop reviews for each Member Entity based on completed workbooks on the BPP online SMART platform;
- regular on-site audits at each of the Member Entities based on the IGC Member Tier and the De Beers selection

For those Member Entities that are RJC Certified Members, i.e. IGC Antwerp and IGC New York, as well as IGC Jewelry and Diamonds (non-Member Entity and business partner), a three-yearly on-site audit is organized by RJC through an independent and internationally qualified auditor.

Depending on the national laws and regulations at the location of the IGC Member Entity, on-site AML/AFC audits are performed by the national government authorities on an ad hoc basis.

6.2.6.3. Financial Accounts Audit

IGC maintains financial records of all its business transactions, which are annually and independently reviewed and certified by a knowledgeable, independent financial auditor. The auditor is appointment without bias or influence.

Each Entity of the IGC Group will act in accordance with national laws and regulations regarding the auditing of its financial accounts and will have its financial accounts independently audited on an annual basis.

7. Records

All IGC Member Entities will keep records on the identification data obtained through the due diligence process, account files, and business correspondence for at least five years after the business relationship ended.

7.1. Data Storage

All IGC Member Entities will retain all necessary records on transactions, both domestic and international, as well as the AML/AFC Activity Reports for at least five years, in a secured location to enable IGC to comply swiftly with information requests from the relevant authorities. Data storage is done in compliance with the GDPR regulations and access is restricted to a limited number of authorized persons.

7.2. Sustained Vigilance

Every IGC Member Entity must remain alert at all time and persistently examine all transactions and facts where money laundering or terrorism financing is suspected, and draw a written report of the examination.

7.3. Updating

For all active customers, suppliers, and business partners, the collected identification data are updated according to the level of the perceived risk.

Any customer, supplier, or other business partner with whom no transactions have been conducted over the past 12 months will be subject to a fresh and integral identification and verification process at the time a new transaction would emerge.

To stay updated with the AML/AFC obligations, a member of the BOD, the GCO and the local Compliance Officer will regularly attend the AML Seminars organized by Antwerp World Diamond Council (AWDC) in Antwerp, Belgium, for which a participation certificate is provided as a reference (copy available in Appendix D).

7.4. Maintenance

All IGC Member Entities will, for at least five years, retain all necessary records on transactions, both domestic and international, in a secured location to enable IGC to comply swiftly with information requests from the competent authorities.

8. IGC Commitment and Implementation

An organization's AML/AFC controls can be easily undermined by a poor culture of compliance. Therefore, IGC supports and maintains a strong AML culture throughout all its Member Entities, enabling to prevent shortcomings, identify issues before they become a concern, and result in more efficient AML/AFC solutions.

Every Director and Manager within IGC is firmly committed to enforce the principles and the policies described above, and compliance with these principles is considered an essential element of IGC's global success and reputation.

The AML/AFC efforts are integrated with a sound understanding across the IGC Member Entities worldwide, allowing to identify and address potential risks in a fast and efficient manner. To achieve the desired goals, the necessary human, financial, and technical resources are made available Group-wide. Resources are regularly reviewed against IGC's size, complexity, and exposure to risk.

At each IGC Member Entity, a Compliance Officer is appointed who reports to the GCO. Because it is important that all managers and employees understand the *what* and *why* of compliance with regard to the activities they undertake, the Compliance Officer and GCO continuously undertake the necessary training and actions to build awareness of IGC's AML/AFT culture and policies throughout the organization.

IGC is incorporating effective AML/AFC controls into its business processes in a way that compliance becomes an integrated part of its daily business practices. Annual internal and external audits enable monitoring the effectiveness of IGC's commitment to help contending money laundering, terrorism financing, and other financial crimes.

Appendix A. Legal Cash Limitations

Updated: November 2019.

BELGIUM (IGC ANTWERP)

Cash limit of maximum **3,000 €**

A maximum of 10% of the transaction price (the amount on the invoice) or the service can be paid in cash. This limitation includes pre-payments and partial payments and no cash transaction may exceed 3,000 euro.

Dealing in cash above this threshold in considered a criminal offense and fines for illegitimate use of cash may be very high.

The cash law of the country in which of with whom the deal is done, applies.

USA (IGCNY– IGCJD)

Businesses as well as individuals who engage in a transaction that results in the transfer of cash as follows:

- over **$10,000**
- received as:
  - a lump sum over $10k
  - two or more related payments in excess of $10k (combined)
  - payments received as part of a single transaction (or two or more related transactions) that exceed $10k in a 12-month period.
- received in the course of trade or business
- from the same person (payer)
- received in a single transaction or two or more related transactions.

HONG KONG (IGCHK – IGCJS)

No legal cash limit. However, where the transaction involves large sums of cash, or is unusual, positive evidence of identity from the sources should be produced; in the case of a foreign national, the nationality should be recorded. Copies of the identification documents should be kept on file.

CHINA (IGC SH)

Yuan-denominated cash transactions exceeding **50,000 yuan** (around $7,100) must be reported to the People's Bank of China (PBOC) (down from the previous level of 200,000 yuan).

In terms of foreign currencies, the report threshold is the equivalent of **$10,000** for both cash transactions and overseas transfers.

THAILAND (SSL)

All cash transactions over **2,000,000 Baht** must be reported

LAO PDR (VDC)

Cash transactions that exceed certain thresholds set by the Anti-Money Laundering Information Office (AMLIO).

BOTSWANA (ZDL)

Currently, no legal thresholds known.

Appendix B. Where to Report

BELGIUM (IGC ANTWERP**)**

The Belgian Financial Intelligence Processing Unit (CFI)
Phone: +32-2.533.72.11
e-mail: info@ctif-cfi.be
or
Antwerp World Diamond Center (AWDC)
e-mail: trst@awdc.be

USA (IGC NY– IGC BS)

U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN")
https://bsaefiling.fincen.treas.gov/main.html

HONG KONG (IGC HK – IGC JS)

Hong Kong Monetary Authority (HKMA)
55/F, Two International Finance Centre, 8 Finance Street,
Central, Hong Kong.

CHINA (IGC SH)

China Anti-Money Laundering Monitoring & Analysis Centre (the "China AML MAC")
Anti-Money Laundering Bureau
Both authorities are within the People's Bank of China (the "PBC")

THAILAND (SSL)

Anti-Money Laundering Office (AMLO)
No. 422 Phayathai Road, Wangmai,
Pathumwan, Bangkok 10330
Phone +66 2219 3600

Email mail@amlo.go.th

LAO PDR (VDC)

Anti Money Laundering Intelligence Office (AMLIO)
Yonnet Rd, Xieng Nyeun Village,
Chanthabouly District, Vientiane, Lao PDR
Phone: +856 21 264624
e-mail: amlio@bol.gov.la

BOTSWANA (ZDL)

Financial Intelligence Agency (FIA)
Attorney General Chambers building - 3rd floor
Gaborone

Appendix C. Definition of Terms

Anti-Money Laundering (AML): AML laws are designed to prevent illegal funds (such as funds obtained from crime, corruption, and tax evasion) from entering the financial system. Financial institutions are required to have procedures in place (such as KYC) to discover high-risk clients, monitor transactions and report suspicious activities (FAFT).

Bribe: A bribe is an illegal payment given or promised in order to induce or influence the judgment or conduct of a person in a position of trust.

Due diligence: Due diligence is a critical element of effectively managing the organizations risks and protecting it against potential financial crimes and nefarious activities. There are two steps in due diligence: (a) understanding the customer activities and (b) assessing the money laundering risk. When onboarding a new customer or if the customer activities substantially change, an analysis of the source of funds and risk associated with those funds is prudent and, in most countries, a legal requirement

Facilitating Payment: A financial payment that may constitute a bribe and that is made with the intention of expediting an administrative process. A facilitating payment is a payment made that acts as incentive to complete some action or process expeditiously, to the benefit of the party making the payment.

Know Your Customer (KYC): KYC is a legal requirement to perform identity checks and do customer due diligence. While KYC laws differ from country to country, the general principle involves collecting enough information to properly identify an individual and ensure that their activities are legitimate (FAFT).

Ultimate Beneficiary Owner (UBO): the UBO of a company refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.” That is to say, you need to know who you are doing business with, the real person (or group of people) who owns or controls that business (FAFT).

Appendix D. AML Seminar Certificate

AWDC ANTWERP WORLD DIAMOND CENTRE

economie

AML & COMPLIANCE SEMINAR
SHORT UPDATE

The **Antwerp World Diamond Centre (AWDC),** in cooperation with

the **Federal Public Service Economy - License Service,**

hereby confirms that **Anne-Marie De Scheemaecker** of the company

Igc Group Nv

has successfully completed the **AML & Compliance Seminar** organized by AWDC

on **10 October 2023**, and has gained knowledge of the anti-money laundering legislation.

(Signature Participant)

Trissia Stavropoulos, Head of Compliance AWDC

Appendix E. AML Training Checklist

IGC MEMBER ENTITY:			
DATE	**NAME**	**ACKNOWLEDGEMENT**	**SIGNATURE**
		I acknowledge that I have read, understood, and accept the IGC Statement on Corporate Integrity.(1)	
		I acknowledge that I have read, understood, and accept the IGC policy on establishing Business Partners (2)	
		I acknowledge that I have read, understood, and accept the IGC statement on Trade-Based Money Laundering (3)	
		I acknowledge that I have read, understood, and accept the IGC statement on Anti-Money Laundering and Anti-Financial Crime (4)	
		I acknowledge that I have read, understood and accept the IGC Governance Framework (5)	
		I acknowledge that I have read, understood and accept the IGC policies and procedures on Bribery and Facilitating Payments (6.1)	
		I acknowledge that I have read, understood, and accept	

		the IGC policies and procedures on Anti-Money Laundering, Anti-Terrorism Financing, and Other Financial Crimes (6.2)	
		I acknowledge that I have read, understood and accept the IGC statement on the Maintenance of Records (7)	
		I acknowledge that I have read, understood and accept the IGC statement on commitment to and implementation of IGC's AML statements, policies, and procedures (9)	
		I acknowledge that I have been properly trained regarding IGC's AML policies and procedures and trained how to contact the IGC Member Entity Compliance Officer and IGC Group Compliance Officer (6.2.5)	