ANTI-MONEY LAUNDERING POLICY

AML POLICY

1. GENERAL PROVISIONS

IGT Company and its future direct and indirect subsidiaries (hereinafter jointly referred to as "the Companies" and severally referred to as "the Company") is an international company operating in various jurisdictions. A reputation for integrity, both in its business behavior and in its management systems, is crucial to Companies' achievement of its commercial goals and to the fulfillment of the corporate responsibilities.

The Company enforces a strict anti-money laundering policy with zero tolerance for money laundering activities. We define money laundering as any activity that is carried out in an attempt to misrepresent the source of funds actually acquired through illegal processes as funds that were acquired through lawful sources/activities.

All IGT Company affiliates are obligated to comply with IGT Company's anti-money laundering policy and with all applicable anti-money laundering laws. Failure to comply can result in severe consequences such as criminal penalties and heavy fines.

The Company ensures complete compliance with laws pertaining to anti money laundering through its related policy.

The Company implements a range of filtration operations for swift and accurate identification of any financial activities that may constitute or are related to money laundering. This helps ensure a money laundering-free financial operations throughout the IGT Company Platform.

Therefore, the Company is committed to the highest standards of Anti-Money Laundering and Combating Terrorism Financing (hereinafter collectively referred to as AML/CTF) compliance and requires management and employees to adhere to these standards to prevent use of the services for money laundering purposes.

The Policy on Prevention of Money Laundering and Terrorist Financing (hereinafter as the «Policy») outlines the general unified standards of internal AML/CTF control which should be adhered to by the Companies in order to mitigate the legal, regulatory, reputational and as a consequence financial risks.

Non-compliance with these laws may lead to serious consequences to the financial condition and reputation of Companies.

2. THE SCOPE AND APPLICABILITY

The Policy is mandatory for all customers.

The customers should do everything in their power to ensure that they are not involved in money laundering and terrorist financing.

All IGT Company customers (further – Customers) acknowledge, undertake and agree to the following terms regarding their opening and maintenance of accounts at IGT Company Platform and for all financial transactions as the IGT Company Platform client:

The Customer will comply (throughout the time as the IGT Company client) with all relevant statutes pertaining to money laundering and proceeds from criminal activities.

3. THE PURPOSE OF THE POLICY

The Policy is designed to comply with the Financial Action Task Force (FATF) standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, AML principles of the Wolfsberg Group, European Directive 2005/60/EC of October, 26, 2005 on the prevention of use of the financial system for the purpose of money laundering and terrorist financing as well as applicable AML/FT laws and regulations of the jurisdictions in which Companies operate with subsequent amendments (the "Applicable Legislation").

The Policy is based on the following legislative acts

Irish Legislation
The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, commenced on 15 July 2010
The Criminal Justice Act 2013, Part 2 amends several sections of the Act
Criminal Justice (Terrorist Offences) Act 2005, Part 4 sets out the definition for terrorist financing

European Legislation
Directive 2005/60/EC - The Third Money Laundering Directive on the prevention of use of the financial system for the purposes of money laundering and terrorist financing

Financial Services Industry Guidelines ("the Guidelines") were published by the Ireland Department of Finance in February 2012 to assist the financial industry in interpreting and effectively complying with their statutory obligations under the Act.

FATF acts and recommendations
The FATF standards include the FATF Recommendations and their Interpretative Notes

The FATF recommendations are recognized as a global standard for combating money laundering (AML) and the financing of terrorism (CFT).

The purpose of the Policy is to provide basic guidance to the Companies and their Employees, wherever located, with regard to major AML/FT requirements.

4. OBJECTIVES

Objectives pursued by this Policy are as follows:

- To prevent criminal elements from using the Companies for money laundering activities;

- Promote a "Know Your Customer" policy as a cornerstone principle for the Companies business practices;

- Conduct self-assessments of compliance with AML policy and procedures.

5. TERMS AND DEFINITIONS

Authorized body means national body (bodies) performing activities aimed at anti-money laundering and counter terrorism financing in accordance with the national legislation and receiving suspicious transactions reports and other reports sent by Company for compliance with national AML/CTF laws and regulations.

Beneficial owner is any individual who I. ultimately owns or controls, whether through direct or indirect ownership or control, more than 25 percent of the shares or voting rights of the client; or II. Otherwise exercises control over the management of the client.

However, if Applicable Legislation or international/cross-border regulations require identifying beneficial owners holding less than 25% or the Company's assessment of the money laundering or terrorist financing risk presented by the customer is high, it may be decided to verify the identities of beneficial owners holding less than 25%.

Client/ Customer means any individual or entity who seeks to enter or has already entered into a business relationship, or conducts a one-off transaction with a Company as principal or as an agent for someone else.

Compliance officer means a person who is in charge of compliance management and/or responsible for AML in the Company.

Employee means an individual working at all levels and grades within Companies, including (but not limited to) the board of directors, the executive board, senior managers, officers, other employees (whether permanent, fixed-term or temporary).

Laundering of proceeds of crime (money) means the making of a legal appearance for the possession, use or disposal of amounts of money or other property received as the result of committing a crime.

Financing of terrorism/Terrorist financing means the providing or raising of funds or the provision of financial services in the knowledge of their being intended for financing an organization, preparing and committing any of the crimes envisaged by Applicable legislation as a terrorist act or for supporting an organized group, illegal military formation or criminal community (criminal organization) that has been formed or is being formed for the purpose of committing any of the said crimes.

Politically Exposed Persons (PEP) means any individuals who are or have been entrusted (domestically or by a foreign country or by an international organization) with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. The definition is not intended to cover middle ranking or relatively junior individuals in the foregoing categories (FATF Guidance on Politically Exposed Persons (Recommendations 12 and 22) from June 2013.)

Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves.

Shell Bank means a bank without a physical presence in any country.

6. RISK-BASED APPROACH (RBA)

6.1. Risk management

A risk-based approach takes a number or all of the following steps in assessing the most cost effective and proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the Companies:

- identify and assess the money laundering and terrorist financing risks that are relevant to the Company;

- design and implement controls to manage and mitigate the assessed risks;

- monitor and improve the effective operation of these controls.

Risk management generally shall be regarded as a continuous process, carried out on a dynamic basis. Companies therefore ensure that their risk management processes for managing money laundering and terrorist financing risks are kept under regular review. It is recommended that the Companies revisit their assessments at least annually.

The general principle of a RBA is that, where there are higher risks, Companies should take enhanced measures to manage and mitigate those risks; and that, correspondingly, where the risks are lower, simplified measures may be permitted (pursuant to Applicable Legislation). In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

6.2. Country Risk

Country risk, in conjunction with other risk factors, provides useful information as to potential money laundering and terrorist financing risks. Country risk is not solely related to the country of origin of a customer. It should also be taken into account that a customer may have business interests in or relevant links to a country that may signify that the customer should be placed in a higher risk category. Factors that may result in a determination that customers from, in or connected with a particular country pose a higher risk includes, for example:

- Countries subject to sanctions, embargoes or similar measures issued by, for example, the United Nations ("UN") or European Union;

- Countries identified by credible sources (e.g. FATF, FATF-style national authorities or other recognized evaluation bodies and EU Commission) as lacking adequate money laundering laws and regulations;

- Countries identified by credible sources as providing funding or support for terrorist activities; or

- Countries identified by credible sources as having significant levels of corruption, or other criminal activity.

6.3. Customer Risk

Determining the potential money laundering and terrorist financing risks posed by a customer, or category of customers, is critical to the development of an overall risk framework. Based on its own criteria, a Company determines whether particular customers pose a higher risk of money laundering and terrorist financing and whether, in some cases, mitigating factors are sufficient to conclude safely that customers engaged in such activities do not, in reality, pose.

Anti-Money Laundering and Counter Terrorist Financing Policy of the IGT Company increases the criteria for money laundering or terrorist financing risks. Application of risk variables may increase or decrease the perceived risk in each case. The application of the variable risk criteria established by the Company in accordance with the requirements of current legislation and international bodies (such as the EU, the FATF, etc.) may increase or decrease perceived risk in each individual case.

The Company conducts proper customer verification to determine whether client or beneficial owner to a foreign PEP and a national PEP or has and, if so, apply additional measures to the usual due diligence of clients (as stipulated in the FATF Recommendations 10, 12, 22)

That measures include:

Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.

Obtaining additional information on the intended nature of the business relationship.

Obtaining information on the source of funds or source of wealth of the customer.

Obtaining information on the reasons for intended or performed transactions.

Obtaining the approval of senior management to commence or continue the business relationship.

Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

The fact that a person is a domestic/international organization PEP does not automatically imply that he/she poses a higher risk.

The Company need nevertheless to be aware of the risks that a PEP may
abuse the financial system to launder illicit proceeds, and need to be aware of the red flags / indicators that can be used to detect such abuse.
Following this, our company uses the risk indicators provided in Appendix 1: PEPs red flags/indicators of the FATF Guidance Politically exposed persons (FATF Recommendations 12 and 22).

The Company will be use outside databases as a tool to assist in the determination of who is a PEP. The Company also may choose to develop in-house databases as a tool to assist in the determination of who is a PEP.

6.4. Product Risk

Certain products and services offered by Companies may pose a higher risk of money laundering or terrorist financing depending on the nature of the specific product or service offered. Such products and services may facilitate a higher degree of anonymity, or involve the handling of high volumes of currency or currency equivalents.

7. CUSTOMER DUE DILIGENCE (CDD) AND KNOW YOUR CUSTOMER (KYC)

7.1. General provisions of Customer Identification

In identifying a customer, the Company obtains a range of information from the customer and verifies this information (or some of it) through the use of reliable, independent source documents, data or information.

As a mandatory part of the CDD process, Companies perform screening of the parties involved against internal and external restricted and black lists.

Companies take reasonable measures to establish, whether the customer is acting for another person or entity and to identify persons to whose advantage the customer acts, except in situations specifically exempted by Applicable Legislation.

The Company take steps to ensure that hold appropriate up-to-date information on their customers. The Company review and update existing customer records based on Company's risk based approach and internal documents not less than once every three years.

The Company operates under certain obligations known as "know-your-client" obligations which grant IGT Company the right to implement anti-money laundering procedures to help detect and prevent money laundering activities where money laundering may mean to handle any funds associated with any illegal activity regardless of the location of such activity.

The Customer agrees to lend full cooperation to IGT Company with respect to anti-money laundering efforts. This involves providing information that IGT Company requests regarding the client's business details, account usage, financial transactions etc. to help IGT Company perform its duties as dictated by Applicable laws regardless of jurisdiction.

The Company reserves the right to delay or stop any funds transfer if there is reason to believe that completing such a transaction may result in the violation of any applicable law or is contrary to acceptable practices.

The Company reserves the right to suspend or terminate any account or freeze the funds in an account if there is reason to believe that the account is being used for activities that are deemed unlawful or fraudulent.

The Company has the right to use client information for the investigation and/or prevention of fraudulent or otherwise illegal activities.

The Company has the right to share client information with:

- a) Investigative agencies or any authorized officers who are helping IGT Company comply with applicable law, including anti-money laundering laws and know-your-client obligations;

- b) Organizations that help IGT Company provide the services it offers its clients;

- c) Government, law enforcement agencies and courts;

- d) Regulatory bodies and financial institutions.

Activities that The Company considers possible indications of money laundering include:

1) The Customer showing unusual apprehension or reservations about IGT Company's anti-money laundering policies.

2) The Customer's interest in conducting financial transactions which are contrary to good business sense or are inconsistent with the client's business policy.

3) The Customer failing to provide legitimate sources for their funds.

4) The Customer providing false information regarding the source of their funds.

5) The Customer having a history of being the subject of news that is indicative of civil or criminal violations.

6) The Customer seems to be acting as a 'front man' for an unrevealed personality or business, and does not satisfactorily respond to requests for identifying this personality or business.

7) The Customer not being able to easily describe the nature of his/her industry.

8) The Customer frequently makes large deposits and demands dealing in cash equivalents only.

9) The Customer maintains multiple accounts and conducts an unusually high number of inter-account or 3rd party transactions.

10) The Customer previously usually inactive account starts receiving a surge of wire activity.

11) The Customer with businesses that handle large amount of cash (i.e. involving €15,000 euros or more, or any currency equivalent) or complex unusually large transactions.

The above list is by no means an exhaustive list.

The Company monitors its client and account activity and takes appropriate measures to prevent money laundering.

7.2. KNOW YOUR CUSTOMER (KYC)

The Customer acknowledges that he/she/it has to complete a KYC check which must be in a form and substance satisfactory to IGT Company. KYC check is carried out by providing necessary information with regard to identification of the Client, beneficial owner and origin of the funds, the scope and type of information depending on the type of Client and the Client amount.

During the Customer's account registration process an individual Customer is providing the

following identification information to the Company:

1) Customer's full name;

2) Customer's date and place of birth and the place of residence or seat;

3) Country of residence/location of customer;

4) Mobile telephone number and e-mail.

During the Customer's account registration process corporate Customer is providing the following identification information to the Company:

1) Full company name;

2) Registration number and date;

3) Country of registration/incorporation;

4) Registered address/office;

5) The names of the director, members of the management board or other body replacing the management board, and their authorization in representing the legal person;

6) Mobile telephone number and e-mail.

After receiving the identification information, the Company's staff should verify this information requesting the appropriate documents.

After receiving the identification information, the Company's staff should verify this information requesting the appropriate documents.

As an identity document:

- a foreign passport (a copy of a spread with a photograph);

- ID card (copies of both sides)

- Driving license (copies of both parties)

- a general passport

Appropriate documents for verifying the identity of Client include, but are not limited to, the requirements which are placed on igt-crypto.io

To verify proof of address of the Client the Company requires one of the following to be provided, in the same correct name of the customer: a high-resolution copy of a utility bill (fixed-line phone, water, electricity) issued within the last 3 months; A copy of a tax or rates bill from a local authority; A copy of a bank statement (for a current account, deposit account or credit card account); A copy of a bank reference letter.

In cases where the client's deposit is 15,000 euros or more, and also if the behavior and transactions

of the client are considered suspicious or risky in relation to the AML policy, the company has the right to request a source of funds. List of documents:

Employment and Other Sources of Income

• any employment confirmation or reference letters that you have or employment contracts (if any) indicating salary and/or bonus

• emolument's certificate

• all documents relating Inheritance/ divorce (including alimony, property settlements, etc.)/ lawsuits/ gifts

• loans agreements certified by Notary or given by Bank

• pension payment

Financial Documents

• complete tax returns

• signed and stamped by bank staff bank statement indicating the transfers of monetary funds related to the primary activity of the Client, from which he has profit

Investments

• brokerage or Asset Management report

• stock certificates

Business Documents

• certified copy of the document confirming that the Client is an individual entrepreneur and that the Client owns a business and copy of the last financial statements

• tax declaration of an individual entrepreneur

Real Estate

• documentation of real estate purchases and sales / valuation for all real estate that the Client owns

• lease documents for real estate from which you earn lease income

The Company has the right to request other documents that will be needed to verify the Customer's compliance or transactions with the requirements of the Company's policies (AML, privacy policy etc.)

The Customer is obliged to collaborate with regard to the KYC/AML check and to provide any information and document deemed necessary by the Company.

The Company may reject any Customer in its sole discretion without being obliged to disclose any

reason for the rejection.

In case the automatic procedures fail, the Company shall contact the Customer by email or other means to obtain the information and documents needed. In case the Customer does not provide the documents in the requested form and any other information requested to satisfy the KYC/AML check within 10 (ten) days, IGT Company may reject the Customer and the costs for the KYC/AML check will be at the cost of the Client.

Additionally, IGT Company has the right to partially or fully withhold the received amounts for any costs or damages incurred by the Company.

7.3. Simplified Customer Due Diligence (SCDD)

For such categories of customer or business as Listed Companies * and Public Authority, a set of SCDD measures reflect the accepted low risk of money laundering or terrorist financing that could arise from such business. Prior to applying SCDD, Companies have to conduct and document appropriate testing to satisfy themselves that the customer or business qualifies for the simplified treatment under this Policy and Applicable Legislation.

**Company listed on a Regulated Market (e.g. the London Stock Exchange Official List) and securities of listed company are admitted to trading on a regulated market.*

7.4. Enhanced Customer Due Diligence (ECDD)

The Companies may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially when the monies are to be paid out into an account other than one in the name of the original applicant and particularly when the proceeds are to be paid to a third party. The examples of customers requiring higher due diligence may include Politically Exposed Persons (PEPs), Correspondent banking institutions, etc.

8. CUSTOMER ACTIVITY MONITORING

8.1. General provisions

The monitoring procedures include types of customer's transactions, the profile of the customer, comparison of the customer's activity and profile with that of a similar, peer group of customers.

8.2. Prohibited Activities

The Company would not do business with

- Anonymous customers;

- Customer is engaged in activity which is deemed to be black listed (e.g. by a regulators);

- The Persons which are currently under any sanctions (international, national, other foreign applicable sanctions).

8.3. Transaction Monitoring

Any information pointing to money laundering or terrorist financing must be reported to the relevant authorities in accordance with the requirements of Applicable Legislation.
The details of transactions prone to AML risks shall be adequately described and a framework for monitoring of transactions and reporting suspicious transactions as well as adequate guidance to staff to recognize suspicious customer behavior shall be outlined in internal documents.

9. REPORTING PROCEDURES

The following core obligations are part of reporting procedures of Company:

- all employees participate in raising information about transactions, which are subject to reporting procedures,

- the Company's Compliance Officer considers all internal reports on transactions subject to reporting procedures and makes an external report to the Authorized body subject to Applicable legislation,

- the details of transactions which are subject to reporting procedures and all correspondence exchanged with the authorities in relation to these transactions are documented,

- the external reports to the Authorized body should contain as much information about the customer, transaction or activity as is determined by national laws and regulations.

A Suspicious Activity Report (SAR) will be made to the Suspicious Transactions Reports Office of the Republic of Ireland (STRO) as soon as the knowledge or suspicion that criminal proceeds exist arises.
The STRO will be responsible for deciding whether or not the suspicion of illegal activity is great enough to justify the submission of a SAR.

10. RECORD KEEPING

All records are kept for at least 5 years and contain records obtained through CDD measures; account files and business correspondence; the results of any analysis undertaken; documents relating to business relations and executed transactions; correspondence with the clients and other persons with whom Companies keeps a business relation.
The five-year period is calculated following the carrying out of the transactions or the end of the business relationship.
The five-year period is calculated following the carrying out of the transactions or the end of the business relationship.
Records of all identity checks will be maintained for up to 5 years after the termination of the business relationship. The business will ensure that all documents, data or information are kept up to date.
Copies of any SAR, together with any supporting documentation filed will be maintained for 5 years from the date of tiling the SAR.
All records will be handled in confidence, stored securely, and will be capable of being retrieved without undue delay.

11. CONFIDENTIALITY AND PERSONAL DATA PROTECTION

The information about customers and their transactions obtained in the course of fulfilling AML/CTF

internal control is considered as confidential.
The employees of the Companies should avoid disclosure to other persons the AML/CTF ways and means implemented by the Company. The "tipping off" is strictly prohibited.

12. TRAINING

One of the most important controls over the prevention and detection of money laundering or terrorist financing is to have employees that are alert to the risks of money laundering/terrorist financing and well trained in the identification of mandatory control transactions and unusual activities or transactions which may prove to be suspicious.
It is recommended that Companies' relevant employees and in particular employees engaged in customer on-boarding, customer servicing, or in settlements receive training at least once a year. Following national laws and regulations, the circle of employees being trained may be broadened.
Extra trainings are given, if AML/CTF laws and regulations or the Company's policies and procedures, as well as new business products and services have materially changed.

13. INTERNAL CONTROL AND AUDIT

The Company improves its AML procedures continuously to monitor unlawful financial schemes.

The Company reserves the right to refuse to process a transaction at any stage, when we believe that the transaction is associated with money laundering or other criminal activity.

The Company complies with the legal requirements of the Republic of Ireland for anti-money laundering. In cases set forth in the relevant legal enactments, we cooperate with officials and government institutions of the Republic of Ireland, as well as other countries.

14. SANCTIONS POLICY

The Company is prohibited from transacting with individuals, companies and countries that are on prescribed Sanctions lists.
The Company will therefore screen against United Nations, European Union, UK Treasury and US Office of Foreign Assets Control (OFAC) sanctions lists in all jurisdictions in which we operate.

15. PROHIBITED JURISDICTION (Jurisdictions with strategic deficiencies)

The Company is prohibited from transacting with individuals, companies and countries that are on prescribed jurisdictions with strategic deficiencies in accordance with the FATF policy
Bosnia and Herzegovina
Ethiopia
Iraq
Sri Lanka
Syria
Trinidad and Tobago
Tunisia
Vanuatu
Yemen
and other jurisdictions according to the prohibitions of the UN, the FATF, or the EU.