

AML/CFT/CFPWMD* HANDBOOK

The aim of this handbook is to set forth policies and risk management procedures that Bravalla B.V. will follow to manage risk and implement controls to prevent its misuse for Money Laundering, Financing of Terrorism, and Financing the Proliferation of Weapons of Mass Destruction (ML/FT/PWMD).

* Anti Money Laundering, Counter Financing of Terrorism, and Counter Financing of the Proliferation of Weapons of Mass Destruction



Introduction

Bravalla B.V. (hereinafter referred to as “Bravalla” or “the Company”). demonstrates an unwavering commitment to conducting its business in strict adherence to the law, particularly those concerning customer due diligence, reporting unusual transactions, and maintaining adequate records (e.g., NOIS, NORUT, Sanctions National Ordinance, Kingdom Sanction Act), unequivocally prohibiting any instances of Money Laundering, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction (hereinafter ML/FT/FPWMD).

This statement represents our policy and it is reflected in the AML/CFT/CFPWMD handbook that was written according to the Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction from the Curaçao Gaming Control Board. The AML/CFT/CFPWMD handbook embodies both the individual and collective commitment of Bravalla's shareholders and Board of Directors against ML/FT/FPWMD. The Board of Directors firmly commits to executing, promoting and internally disseminating the policies outlined in this handbook and other compliance procedures as well as maintaining the institutional and financial capacity necessary to ensure that procedures remain current and adequate for risks mitigation.

In addition to the Company's existing codes, policies, and procedures related to Anti-Money Laundering, Countering the Financing of Terrorism, and Countering the Financing of Proliferation of Weapons of Mass Destruction (hereinafter AML/CFT/CFPWMD), this handbook serves as tool to emphasize our Zero Tolerance for ML/FT/FPWMD. Through this document, we delineate the core components of our corporate program designed to prevent the associated risks and describe risk management steps to address ML/FT/FPWMD risks.

This handbook remains subject to updates, which may occur due to changes in processes, decisions by the Board of Directors, audit reviews, alterations in the institution's business model, or any other circumstances deemed relevant. The content of this handbook includes policies and procedures according to the Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction



from the Curaçao Gaming Control Board, any reproduction or alteration without following the correspondent steps and communication procedures is prohibited. This handbook and the information contained herein is the property of Bravalla B.V. Any reproduction of its content is prohibited except as authorized in writing by Bravalla B.V.

Regards,

Bravalla's Board of Directors

Definitions

Casino: online casinos.

CFATF: Caribbean Financial Action Task Force, an organization of 24 states in the Caribbean Basin, Central and South America, implementing common countermeasures against money laundering.

Compliance Officer: A senior officer at management level, independent from gaming operations, responsible for detecting and deterring money laundering and terrorist financing.

FATF: Financial Action Task Force, an independent intergovernmental body established in 1989 to develop and promote policies to protect the global financial system against money laundering, terrorist financing, and the financing of weapons of mass destruction.

FATF Recommendations: A framework of policies and measures issued by FATF to combat money laundering, terrorist financing, and the financing of weapons of mass destruction.

Financial Transactions: In casinos, these include purchasing or cashing in casino chips or tokens, opening accounts, wire transfers, and currency exchanges, excluding gambling transactions with only casino chips or tokens.

FIU: Financial Intelligence Unit Curaçao, as referred to in art. 2 of the NORUT.

Kingdom Sanctions Act: National Ordinance known as "Rijkssanctiewet," published under N.G. 2016 no. 54.

NOIS: National Ordinance on Identification of Clients when rendering Services (Landsverordening identificatie bij dienstverlening, N.G. 2017, no. 92).

NORUT: National Ordinance on the Reporting of Unusual Transactions (Landsverordening Melding Ongebruikelijke Transacties, N.G. 2017, no. 99).



Other Online Games: Includes sports betting, esports betting, fantasy sports, lottery, bingo, skill-based games, and virtual sports.

Politically Exposed Persons (PEPs): Could refer to any of the following definitions

Foreign PEPs: Individuals with prominent public functions by a foreign country, including their family members and close associates.

Domestic PEPs: Individuals with prominent domestic public functions.

International Organization PEPs: Senior management members of international organizations.

Sanctions National Ordinance: National Ordinance known as "Sanctielandsverordening," published under N.G. 2014 no. 55.

Source of Funds: How the funds for a particular transaction were obtained (e.g., savings, pension, property sales, dividends, winnings, gifts, legal compensation).

Source of Wealth: The origin of all the money a person has accumulated (e.g., employment income, inheritances, investments, business ownership).

Unusual Transaction: A transaction considered unusual based on certain indicators, pursuant to Article 10 of the NORUT.

Ultimate Beneficial Ownership (UBO): Refers to the natural person(s) who ultimately own(s) or control(s) a customer or on whose behalf a transaction is conducted, including those exercising ultimate control over a legal entity.

Money laundering

Money laundering is a process through which individuals or entities attempt to make illegally obtained funds, often referred to as "dirty money," appear legitimate or "clean." This illegal activity involves a series of financial transactions and activities that obscure the origins of the illegal gains, making it difficult for law enforcement and authorities to trace the money back to its criminal source.

Money laundering typically consists of three main stages:

Placement: In this stage, the illicit funds are introduced into the financial system. This can involve depositing cash into online gambling accounts, to get the money into the legitimate economy.

Layering: after converting the cash into an electronic balance, the money launderers create a complex web of transactions and financial activities to distance the funds from their source. They may move money between various accounts, conduct multiple transfers, or engage in international transactions to make it difficult to trace the money's origins.

Integration: In the final stage, the "cleaned" funds are reintroduced into the legitimate economy. This can involve investing in legal businesses, purchasing assets like real estate, or using the funds for personal expenditures. At this point, the money appears to be legitimate and free from any association with criminal activities.

Financing of terrorism

Refers to the process of providing financial support to terrorist organizations, individuals, or activities in order to facilitate acts of terrorism. This support can come in various forms, including the provision of funds, resources, assets, or even logistical assistance. The primary purpose of financing of terrorism is to enable terrorists to carry out their activities, such as planning and executing acts of violence, with the goal of promoting a

particular ideology, destabilizing governments, or causing fear and terror in society. Money laundering techniques are frequently employed to obscure the source of funds and make them appear legitimate. Terrorist financiers often use money laundering to evade detection by authorities.

Financing of the proliferation of weapons of mass destruction

Refers to the financial support provided to individuals, organizations, or states involved in the development, acquisition, or dissemination of weapons of mass destruction. Weapons of mass destruction include nuclear, chemical, biological, and, in some cases, radiological weapons that have the potential to cause significant destruction, casualties, and harm on a large scale. Proliferation financing can take various forms and plays a crucial role in enabling the spread of these dangerous weapons. Money laundering methods are also commonly utilized to conceal the origin of funds used for financing of the proliferation of weapons of mass destruction and give them an appearance of legitimacy.

Unscrupulous individuals use legal gambling operations to introduce illegal money into the economic systems. Money laundering is a serious criminal offense. Bravalla helps to disrupt the process and prevent criminals from enjoying the profits of their illegal activities by implementing an Anti-Money Laundering (AML), Countering the Financing of Terrorism (CFT), and Countering the Financing of Proliferation of Weapons of Mass Destruction (FPWMD) controls.

1. Who does this handbook apply to?

Bravalla's board of directors, officers, managers, employees, independent contractors, consultants, counsels, agents, and representatives.

2. What does Bravalla expect from you?

Bravalla's expects you to carefully review and grasp the contents of this Handbook.



3. Objective

Bravalla's board of directors, employees, officers, managers, employees, agents, contractors, and individuals representing the interests of the company must refrain from engaging in any ML/FT/FPWMD activities, irrespective of their nationality, residence, or location.

Furthermore, it is imperative that the Compliance Officer, and operations departments, efficiently carry out the program detailed in this handbook.

TABLE OF CONTENTS

INTRODUCTION	2
DEFINITIONS	4
MONEY LAUNDERING	6
<i>Placement:</i>	6
<i>Layering:</i>	6
<i>Integration:</i>	6
FINANCING OF TERRORISM	6
FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION	7
1. WHO DOES THIS HANDBOOK APPLY TO?	7
2. WHAT DOES BRAVALLA EXPECT FROM YOU?	7
3. OBJECTIVE	8
1. INTERNAL STRUCTURES	11
1.1 ROLES AND RESPONSIBILITIES OF THE COMPLIANCE AREA	11
1.1.1 <i>Board of directors (BofD)</i>	11
1.1.2 <i>Money Laundering Reporting Officer (MLRO)</i>	11
1.1.3 <i>Fraud and Payments Team - Transaction Monitoring Area</i>	11
1.1.4 <i>Operations Team</i>	11
2. AML/CFT/CFPWMD COMPLIANCE PROGRAM	13
2.1 A SYSTEM OF INTERNAL POLICIES, PROCEDURES, AND CONTROLS	14
2.2. APPOINTMENT OF A COMPLIANCE OFFICER	14
2.3 EMPLOYEE SCREENING PROGRAM AND ONGOING TRAINING PROGRAM	15
2.4 INDEPENDENT AUDIT FUNCTION TO TEST THE AML/CFT/CFPWMD PROGRAM	16
<i>Examination by the Gaming Control Board</i>	16
3. RISK MANAGEMENT PROCESS	17
4. RISK FACTORS AND CONTROLS	19
CUSTOMER RISK ASSESSMENT (CRA)	19
PROCEDURES, AND CONTROLS	19
RISK FACTORS SPECIFIC TO THE GAMBLING SECTOR	20
<i>Customer Risk</i>	20
<i>Geographical Risk</i>	21
<i>Product, Service, and Transaction Risk</i>	23
<i>Distribution Channels Risk</i>	24
CUSTOMER DUE DILIGENCE (CDD)	25
<i>Introduction</i>	25
<i>Identification and Verification of the Player</i>	26
<i>Conduct a Customer Risk Assessment</i>	27
<i>Sanctions and status screening</i>	28
<i>Identification and Verification of the Beneficial Owner</i>	28
<i>Obtaining Information on the Purpose and Intended Nature of the Business Relationship</i>	29



ONGOING MONITORING	30
<i>Ongoing Monitoring of Identity:</i>	30
<i>Ongoing Monitoring of Transactions:</i>	30
<i>Timing of CDD Measures</i>	31
<i>Enhanced Due Diligence</i>	35
POLITICALLY EXPOSED PERSONS (PEPs)	35
APPLICATION OF CDD MEASURES TO EXISTING CUSTOMERS	37
TERMINATION OF THE BUSINESS RELATIONSHIP	37
REPORTING OF UNUSUAL TRANSACTIONS	38
<i>Reporting Obligations</i>	38
<i>The Documentation of Unusual Transactions</i>	39
<i>Prohibition of Disclosure</i>	39
<i>Record Keeping</i>	39
ANNEX A.	41

1. Internal Structures

1.1 Roles and Responsibilities of the Compliance Area

1.1.1 Board of directors (BofD)

Board of Directors is the governing body of Bravalla, whose members are elected by shareholders to set ML/FT/FPWMD risk management strategy, oversee management, and protect the interests of shareholders and stakeholders.

Board of Directors must promote approve and internally coordinate the dissemination of the policies outlined in this handbook and other compliance procedures as well as maintaining the institutional and financial capacity necessary to ensure that procedures remain current and adequate for risks mitigation.

1.1.2.Compliance Officer

Responsible for the implementation of the established strategies, as well as assessing regulatory, legal and product risk-based needs, in order to ensure that the operation complies with current legislation and do the unusual activity report. Additionally, he must assess the inherent risks and impacts of new products, services and technologies that the company intends to implement, which will then be presented to the Compliance Committee.

1.1.3 Fraud and Payments Team – Transaction Monitoring Area

This team is responsible for monitoring customer transactions (whether deposits, withdrawals or intra-systemic transactions) in accordance with the company's handbook policies and procedures, as well as applicable legislation and other good practices.

1.1.4 Operations Team

This team is responsible for rendering casino and sportsbook services.



2. AML/CFT/CFPWMD Compliance Program

An AML/CFT/CFPWMD program is a critical component of a casino's compliance framework. Its primary goal is to protect the organization from money laundering activities and ensure full compliance with relevant laws and regulations. Therefore, designing, structuring, and implementing these programs should be top priorities for any gambling operator.

An AML/CFT/CFPWMD program is risk-based and tailored to mitigate the specific money laundering, terrorist financing and financing of the proliferation of weapons of mass destruction risks the organization may face. This program establish minimum standards that comply with applicable laws and regulations and be supplemented by the institution's policies and procedures.

Understanding the legal requirements for institutions, employees, and customers in Curaçao is essential before designing an AML/CFT/CFPWMD program.

Key elements of an AML compliance program include:

1. A system of internal policies, procedures, and controls.
2. A designated compliance officer with day-to-day oversight of the AML/CFT/CFPWMD program.
3. An employee screening and ongoing training program.
4. An independent audit function to test the AML/CFT/CFPWMD program.
5. The AML/CFT/CFPWMD program should also ensure compliance with obligations regarding customer due diligence, reporting unusual transactions, retention periods, data protection, and training that will be addressed in the third chapter of this handbook.

Bravalla should systematically test and adapt the AML/CFT/CFPWMD program to address current risks within the organization, with approval from senior management.

Bravalla will ensure that their foreign branches and subsidiaries, if any, implement AML/CFT/CFPWMD measures consistent with Curaçao's requirements.

2.1 A System of Internal Policies, Procedures, and Controls

Bravalla has policies and procedures, including but not limited to a policy statement expressing senior management's commitment to combating the misuse of facilities, products, and services for money laundering, terrorist financing, and the proliferation of weapons of mass destruction, included in page 2 of this handbook.

Standard AML operating procedures, more detailed than policies, translate policy into acceptable and workable practices.

Bravalla will have processes to stay updated on regulatory changes to keep their programs current. Internal controls should enable the compliance officer to recognize deviations from standard procedures and protocols. The policies and procedures should be in writing and approved by the board of directors and communicated to employees.

2.2. Appointment of a Compliance Officer

Bravalla will designate a senior officer at management level, independent from gaming operations, responsible for detecting and deterring money laundering and terrorist financing. The AML/CFT/CFPWMD compliance officer must have timely access to customer identification data, transaction records, and other relevant information and must be able to act independently.

Responsibilities include:

- Designing and implementing the AML/CFT/CFPWMD program.
- Ensuring compliance with local laws and regulations.
- Reviewing adherence to Bravalla's policies and procedures.
- Organizing staff training on compliance-related issues.
- Analyzing transactions and verifying those subject to reporting.
- Reviewing internally reported unusual transactions.
- Keeping records of reported unusual transactions.
- Conducting closer investigations of unusual transactions.
- Preparing external reports of unusual transactions.
- Updating the AML/CFT/CFPWMD program as needed.

- Staying informed on developments in money laundering and terrorist financing.
- Preparing periodic reports on AML efforts.
- These responsibilities should be included in the compliance officer's job description, signed, and dated by the officer.

2.3 Employee Screening Program and Ongoing Training Program

Bravalla will ensure high ethical standards and compliance with financial transaction laws and regulations.

Bravalla will develop and provide training programs for all personnel handling transactions that may be deemed unusual based on the indicators outlined in the Ministerial Decree regarding the Indicators for Unusual Transactions. Training should cover rules of conduct, ongoing education on AML policies, and should be tailored to different segments of the institution. Training must address:

1. New employees: General training on money laundering and terrorist financing, internal policies, customer due diligence, and reporting requirements.
2. Operations personnel: Training on recognizing and responding to potential money laundering activities.
3. Audit staff: Training on regulatory changes, money laundering methods, and their impact.
4. Fraud and Payments Team – Transaction Monitoring Area: Specialized training to stay updated on trends and changes.
5. Supervisors and managers: Comprehensive training on AML policies, procedures, and regulations.
6. Board of directors: Regular communication on money laundering risks.

Refreshment training should be provided regularly to keep staff informed of developments. Records of training, including content, attendees, dates, and results, must be maintained.

2.4 Independent Audit Function to Test the AML/CFT/CFPWMD program

The AML compliance program must be monitored and evaluated annually by an internal audit department or an outside independent party. The audit should be independent, conducted by individuals not involved in the Fraud and Payments Team - Transaction Monitoring Area and compliance staff, and include:

- Evaluation of AML, counter-terrorist financing, and counter-proliferation manuals.
- Customer file review.
- Compliance management assessment.
- Transaction testing.
- Training adequacy assessment.
- Compliance with laws and regulations.
- System's ability to identify unusual activity.
- Employee and supervisor interviews.
- Sampling of unusual transactions and compliance review.
- Record retention system adequacy assessment.
- The audit findings must be documented, and deficiencies reported to senior management and the Board of Supervisory Directors for prompt corrective action.

Examination by the Gaming Control Board

Bravalla must provide information or documentation on their AML/CFT/CFPWMD policies and procedures to Gaming Control Board examiners upon request. This includes:

The written and approved AML Compliance Program.

Business Risk assessment records.

Compliance Officer's name and job description.

Records of reported unusual transactions and investigations.

Records of frozen accounts.

Training schedules.

Internal or external audit assessment reports.

Customer files, including risk assessments, due diligence, acceptance, and transaction information.

3. Risk Management Process

Bravalla demonstrates a commitment to systematic AML/CFT/PWMD risk management practices. This structured approach enables the organization to identify, assess, and respond to risks in a proactive and strategic manner, ultimately enhancing its ability to achieve its objectives and sustain long-term success.

Below, you will encounter an introductory overview of the comprehensive explanation that awaits within this chapter.

Establishing Context: This initial step involves defining the scope, objectives, and parameters of the risk management process. It entails identifying internal and external factors that could impact the organization's ability to achieve its goals. By understanding the context in which risks arise, the company can effectively tailor its risk management strategies.

Risk Assessment: this step encompasses three steps; identification, analysis and evaluation.

Risk Identification: In this phase, the organization systematically identifies potential risks that could affect its objectives. This encompasses both internal risks, such as operational inefficiencies or resource limitations, and external risks, including market fluctuations or regulatory changes. Thorough identification allows for a comprehensive understanding of the risk landscape.

Risk Analysis: Once risks are identified, they are analyzed in terms of their likelihood and potential impact on the organization. This step involves assessing the

likelihood of each risk occurring and estimating the magnitude of its consequences. Through quantitative and qualitative analysis techniques, the company can prioritize risks based on their severity and likelihood of occurrence. Risk Evaluation: Following analysis, risks are evaluated to determine the level of acceptability or tolerability to the organization. This involves comparing the assessed risks against predefined risk criteria and risk appetite thresholds. Risks that exceed acceptable thresholds may require mitigation strategies, while those within acceptable limits may be monitored or accepted without further action.

Risk Treatment: In this stage, the company develops and implements risk controls and treatment plans to address identified risks. Treatment options may include risk avoidance, mitigation, or transfer depending on the nature and severity of the risk. Through effective treatment, the organization aims to reduce the likelihood or impact of adverse events and enhance its resilience to risk.

Recording and reporting: Risk recording and reporting refers to the process of systematically identifying, documenting, and communicating risks within an organization. It involves keeping track of all risk management steps and reporting this information to relevant stakeholders and when needed to the authorities according to legal requirements.

Monitoring and Review: Risk management is an ongoing process that requires continuous monitoring and review. This involves tracking the effectiveness of implemented risk treatments, assessing changes in the risk landscape, and updating risk management strategies accordingly. By maintaining vigilance and adaptability, the company can proactively address emerging risks and optimize its risk management approach.

Communication and Consultation: Throughout the risk management process, effective communication and consultation are essential. This entails sharing relevant risk information with stakeholders, fostering a culture of risk awareness and accountability, and soliciting input from internal and external sources. Open communication channels facilitate informed decision-making and promote organizational resilience.

4. Risk factors and controls

Customer Risk Assessment (CRA)

Before conducting any occasional transactions or establishing a business relationship, a personalized risk assessment of the customer must occur. This assessment may need revisiting as the business relationship progresses, potentially leading to adjustments in the customer's risk rating.

The Customer Risk Assessment evaluates the specific risks Bravalla faces in providing services to players.

The data collected for the CRA helps create a customer's risk profile. Based on this assessment, the appropriate level of Customer Due Diligence (hereinafter referred to as CDD) can be applied in accordance with the Customer Acceptance Policy (CAP). Hence, the Company will adopt a Customer Acceptance Policy outlining:

- Descriptions of player types posing higher ML/FT/FP risks
- Risk indicators categorizing risks
- Levels of Customer Due Diligence (CDD), including ongoing monitoring
- Circumstances under which service may be declined

When formulating CAP, we will adhere to obligations concerning Politically Exposed Persons (PEP) and Sanctions Screening.

Procedures, and Controls

Bravalla will uphold the policies established in this handbook, and will draft more procedures, and controls to effectively mitigate and manage risks associated with money laundering, terrorist financing, and proliferation of weapons identified in the operator's risk assessment.

Measures to mitigate ML/FT/FP risks should encompass:

- Customer Due Diligence (CDD)
- Record-keeping protocols
- Reporting procedures
- Risk management measures including Customer Acceptance Policies (CAP), Customer Risk Assessment (CRA) procedures, internal controls, compliance management, communication of policies and controls, employee training, and employee screening policies and procedures.

These measures need clear documentation and approval by the Board of Directors. Bravalla will monitor their implementation and enhance them if needed, especially in areas where higher risks are identified.

Risk Factors Specific to the Gambling Sector

Within the gambling sector, there are four key areas that need to be addressed in both business risk assessment and customer-specific risk assessment:

Customer Risk

Customer risk refers to the potential for money laundering (ML) or terrorist financing (TF) associated with maintaining relationships with certain individuals.

This risk assessment typically relies on factors such as the individual's economic activity and source of wealth. Categories of customers posing higher risks include those with:

1. Multiple income sources
2. Irregular income streams
3. Politically Exposed Persons (PEPs)
4. High spenders with potentially illicit sources of money
5. Disproportionate spenders compared to known income/assets
6. Customers with spending patterns abrupt changes

7. Use of third parties to evade due diligence measures
8. Multiple casino player rating accounts to obscure gambling activities
9. Unknown customers redeeming large amounts
10. Junkets, which monitor player activity and credit issuance
11. Casinos establish a benchmark representing typical player transaction values. A player with a single, steady income source poses lower ML/TF risk than one with multiple or irregular income streams.

Geographical Risk

Geographical risk pertains to the risk associated with a player's location and the source of wealth in the business relationship. Factors such as nationality, residence, and place of birth are considered, as they may indicate heightened risk. High-risk countries include those with weak anti-money laundering/counter-terrorism financing (AML/CFT) systems, significant corruption, international sanctions related to terrorism or weapons proliferation, and known terrorist activity. Reliable sources for assessing geographical risk include:

FATF lists of high-risk jurisdictions and those under increased monitoring
CFATF Public Statement
U.S. Department of State's INCSR
European Commission's list of countries with AML/CFT deficiencies
OFAC sanctions
Credible sources identifying funding or support for terrorism
Transparency International's Corruption Perception Index

Bravalla instrumentalizes the country rating tool provided by www.knowyourcountry.com to determine the geographic area risk.

This rating tool offers a comprehensive assessment of risk factors related to money laundering, terrorism financing, corruption, international sanctions, criminality, resilience against organized crime, and offshore financial activities. It provides a structured approach to evaluating and comparing countries based on these key indicators, helping



users make informed decisions regarding investment, business operations, and compliance.

Here's a breakdown of the weighted indicators:

Money Laundering/Terrorist Financing Risks (52.5%):

Comprises four sub-indicators:

FATF Uncooperative/AML Deficient (Weighting: 20)

FATF Compliance with 40+9 Recommendations (Weighting: 15)

US State ML Assessment (Weighting: 7.5)

US Secretary of State Terrorism (Weighting: 10)

International Sanctions (15%):

Focuses on the imposition of sanctions by international bodies such as the UN, US (OFAC), and EU.

Corruption Risks (7.5%):

Reflects the perceived risk of corruption within a country, based on Transparency International's Corruption Perception Index and the World Bank's Governance Indicators.

Global Initiative Criminality Index (10%):

Measures criminality on a country-by-country basis, covering various criminal markets and actors.

Global Initiative Resilience Index (5%):

Evaluates a country's resilience against organized crime, considering factors such as political leadership, government transparency, and international cooperation.

EU Tax Blacklist (5%):

Identifies countries listed on the EU Tax Blacklist or Greylist.

Offshore Finance Centre (5%):

Identifies countries classified as Offshore Finance Centres or Conduits.

Bravalla renders services for people located in Brazil.

Brazil currently has a score of 68.7 out of 100 for its Anti-Money Laundering (AML) compliance, with 100 representing the highest level of compliance. This corresponds to a medium level of risk.

The geographical factor in risk analysis transcends mere national boundaries, delving into the intricate landscape of specific regions or states within countries. These regions and states, often characterized by unique socio-economic dynamics and environments, harbor pockets of vulnerability that amplify the risk of ML/FT/FPWMD.

Border cities in Brazil present a higher risk of organized crime presence, those listed according to the IBGE will be considered to analyze inherent risk.

Also the states with the highest ML/FT/FPWMD crime rates are present in studies carried out jointly by CNJ (Conselho Nacional de Justiça) and INSPER (Instituto de Ensino e Pesquisa), and therefore have a high risk in our risk analysis.

For control purposes, the factor will initially be assigned on the basis of the person's registration file, then it will be reviewed once we request the Proof of Address.

Product, Service, and Transaction Risk

Certain products, services, and transactions present higher inherent risks and are more attractive to criminals. These include gaming products allowing player influence over game outcomes and payment methods vulnerable to ML/TF. High-risk factors include:

1. Proceeds of crime
2. Cash transactions facilitating the exchange of illicit funds
3. Anonymous payment methods like prepaid cards and virtual assets
4. Misuse of casino accounts
5. Specific games susceptible to exploitation
6. Peer-to-peer gaming
7. Use of third-party accounts or cards
8. Funds transfer between gaming accounts
9. Certain financial services (e.g., credit, currency exchange)

10. Multiple casino accounts or wallets
11. Identity fraud
12. Funding prepaid cards with cash
13. Games involving multiple operators
14. E-wallets, particularly unlicensed ones or those accepting cash deposits

The company's website showcases two primary verticals: sports betting and casino games. It is noteworthy that the casino games offered at KTO.COM are sourced from licensed game service providers, all of which possess accreditations from reputable laboratories. Consequently, when assessing the risk associated with the casino offerings, controls derived from laboratory certificates and compliance programs are duly considered.

In contrast, sports betting and live casinos lack such automatic preventive controls coming from laboratories, thus representing a higher inherent risk sub-factor.

Our commitment for preventing criminals from exploiting our company and the gambling industry to commit fraud is the reason why the company has chosen to manage the risk arising from lack of integrity when betting, in order to make this process easier the company decided to become a member of integrity associations.

KTO is proud to be part of the International Betting Integrity Association (IBIA hereinafter). IBIA has a Monitoring & Alert Platform that is a highly effective anti-corruption tool. This platform detects and reports suspicious activity on IBIA members' betting markets. IBIA has longstanding information sharing partnerships with leading sports bodies including FIFA, UEFA, ITIA and the IOC and many gambling regulators to utilize this data and prosecute corruption, which is a source crime for money laundering.

Distribution Channels Risk

The on-line channels impact risk profiles. Sub-factors affecting risk include anonymity, non-face-to-face interactions, and involvement of third parties without AML/CFT obligations.



Bravalla will establish procedures and controls to prevent technological advancements from being exploited for money laundering or terrorist financing purposes by identifying its customers.

Risk assessments Bravalla are necessary when introducing new products, business practices, delivery mechanisms, or technologies to identify and mitigate potential weaknesses that could be exploited by criminals. These assessments must be documented, and mitigation measures implemented where risks are identified.

Customer Due Diligence (CDD)

Introduction

Bravalla is prohibited from maintaining anonymous or obviously fictitious accounts. To establish or maintain a business relationship or conduct occasional transactions, Bravalla will ascertain the player's identity and gather relevant information to understand the purpose and nature of the relationship.

Implementing a Customer Due Diligence (hereinafter referred to as CDD) program is crucial for preventing money laundering, terrorist financing, and proliferation financing.

Understanding the customer's risk profile enables Bravalla to tailor its CDD measures to mitigate identified ML/TF risks. The primary objective of collecting information is to furnish Bravalla with documentation for risk assessment associated with the player and to develop a customer profile to anticipate their behavior within the business relationship. This assessment is vital for detecting any deviations from expected behavior, with any anomalies requiring reporting to the Financial Intelligence Unit (FIU).

Bravalla is obligated to conduct Customer Due Diligence measures when:

- a. Players engage in financial transactions equal to or exceeding NAf. 4,000;

- b. Occasional transactions surpass the monetary equivalent of NAf. 4,000;
- c. There is suspicion of money laundering or terrorist financing; or
- d. Doubts arise regarding the veracity or adequacy of previously obtained customer identification data.

Note: A transaction can constitute a single occurrence or a series, combination, or pattern of transactions amounting to a total exceeding the monetary equivalent of NAf. 4,000.

Transactions are deemed interconnected if, for instance, they are conducted by the same player through the same game or within a single gaming session. In such instances, it is expected to apply CDD measures outlined below. Here, Bravalla will identify the player, conduct a customer risk assessment, and verify the player's identity. Whenever an occasional transaction poses a high ML/TF risk, enhanced due diligence measures must be implemented.

Bravalla B.V. does not use physical establishments and therefore risk coming from this source is not assessed.

Identification and Verification of the Player

Identification involves collecting personal details of the player to establish their identity, while verification confirms these details using reliable, independent source documents, data, or information. The extent of information required and verification varies based on risk.

Identification of the player: At a minimum, the following information must be collected:

1. Full name
2. Permanent residential address
3. Date of birth
4. Place of birth
5. Nationality
6. Identity number

However, in low-risk scenarios, gambling operators are allowed to limit identification to the three personal details mentioned in points 1 to 3 above. Conversely, in high-risk situations, the operator may consider it necessary to collect additional personal details to mitigate the increased risk of ML/FT/FPWMD.

Conduct a Customer Risk Assessment

This step is essential to gather sufficient information to detect unusual activity during the business relationship. A provisional risk rating is assigned based on the initially collected information, which is revised once additional questions are answered or more information is received. Based on the CRA, the appropriate level of CDD can be applied as stipulated by the CAP.

Verification of identity refers to the actions taken to confirm that a person exists and is who they claim to be. This is done by checking reliable, independent sources (separate from the person whose identity is being verified).

Typically, identity verification involves referencing an unexpired government-issued document containing photographic evidence of the customer's identity (e.g., passport, identity card). If such a document does not verify the player's residential address, Bravalla may obtain other documents such as a bank statement, utility bill, letter from a public authority, or rental agreement, which should be no more than six months old.

Bravalla can also contact the player via letter, email, or telephone to verify the provided information, or send a verification code to the email address to confirm its validity. Verification can also involve checking social media, telephone directories, company registries, or media sources. Biometric checks can confirm that the individual presenting the document matches the person described therein. Additionally, Bravalla may cross-reference the information with geo-location data, IP address data, funding method data, etc.

Verification ensures that Bravalla is satisfied that the player is who they claim to be. It is important that documents are clear, legible, and of good quality. Verification of identity

evidence includes checking the legitimacy of the document and ensuring it has not been stolen.

If the Bravalla is not sufficiently confident in a player's identity, additional measures should be taken. These measures may include requesting further identification documents, asking the player to provide a photo of themselves holding their ID, requiring a first payment through an account in a reputable jurisdiction, using systems that generate codes sent to a verified mobile phone, and requiring these codes to be returned.

Sanctions and status screening

All players should be screened against sanctions lists from the UN and EU. If Curaçao publishes a local list of designated persons and organizations, Bravalla should also consider this list.

By using sanction list checking Bravalla ensures the company does not engage with customers subject to international sanctions. Before conducting business or performing an occasional transaction with a player for the first time, the casino should check published lists of known or suspected terrorists or other sanctioned persons or companies, such as the U.S. Treasury's Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons List.

For PEP status screening, Bravalla can rely on internet searches or consult reports and databases on corruption risk, such as the Transparency International Corruption Perceptions Index or www.knowyourcountry.com.

Identification and Verification of the Beneficial Owner

Bravalla is required to identify and verify the identity of the beneficial owner. Bravalla should ensure that customers are registering accounts to play and transact on their behalf.



This target is achieved by including specific wording in the terms and conditions that a potential player is representing registering an account to play and transact on their behalf.

Bravalla's business model exclusively accepts individual customers, thereby precluding the registration of corporate accounts or legal entities. The automated registration process for individual accounts eliminates the necessity for procedures pertaining to the identification and verification of Ultimate Beneficial Owners associated with legal entities as it is not possible to create an account without a real individual personal information, including but not limited to the national identification number CPF.

Obtaining Information on the Purpose and Intended Nature of the Business Relationship

One of the requirements of CDD is for subject persons to understand why a prospective customer seeks a specific service or product.

In the gambling sector, the purpose of opening a gaming account is often evident, so casinos typically do not need additional information from customers. However, CDD measures also require developing a customer risk profile to detect unusual activity during the business relationship.

Bravalla will collect sufficient information and, when necessary, documentation to establish a customer's source of wealth and the expected level of activity. The source of wealth involves determining the activities that generate the customer's net worth and whether this justifies the projected and actual account activity levels. The extent of information collected should reflect the ML/FT/FPWMD risk level identified through the customer risk assessment.

In low-risk scenarios, a customer's declaration with some details (e.g., nature of employment/business, usual annual salary) may be sufficient.

Social media can also be used as an information source. In higher-risk scenarios or if there are doubts about the information's accuracy, the information must be substantiated by independent and reliable sources and documentation. To develop a customer risk profile, Bravalla may also use statistical data to create behavioural models to gauge a customer's



activity instead of collecting source of wealth information. If this approach is chosen, data from sources like the Central Statistics Department can help determine the average wagering power of players from a given jurisdiction.

Data collected by Bravalla over time can also create the profile of an average player. This method should only be used when the customer base is large enough to develop an average profile.

It is important to note that using statistical data is incompatible with high-risk situations since the transactional pattern will fall outside the average behavioral model. In such cases, Bravalla will collect source of wealth information as described above.

Ongoing Monitoring

Bravalla will conduct ongoing due diligence on the business relationship and scrutinize transactions to ensure they are consistent with the knowledge about the customer, their business, and risk profile.

Ongoing Monitoring of Identity:

Bravalla will maintain accurate and up-to-date identification data. Since identity may change over time. This may involve periodically obtaining identity evidence, refreshing data at key events (e.g., change of payment instrument), or tracking the expiry dates of identity documents.

Bravalla will assess if changes are substantial enough to require a reassessment of the customer's risk.

Ongoing Monitoring of Transactions:



Transaction monitoring aims to prevent involvement in ML/TF activities. If transactions are inconsistent with Bravalla's expectations or knowledge of the customer, Bravalla will investigate the unusual activity and, if necessary, establish the source of funds for the transaction. Understanding deviations in transactions may require sufficient information and documentation. The customer's risk profile may need to be revised based on the information received. Bravalla will decide whether the transaction is unusual and needs to be reported to the FIU.

The level of ongoing monitoring depends on the customer's risk profile, but even low-risk situations require some degree of oversight to ensure the business relationship remains low risk.

Timing of CDD Measures

Bravalla will conduct identity verification when engaging in financial transactions equal to or exceeding NAf. 4,000. All CDD measures will be completed by the time this threshold is reached.

The threshold above will be calculated daily, including all deposits and withdrawals since the business relationship began. Upon reaching the threshold, Bravalla will conduct PEP status screening, perform a customer risk assessment, and fulfill remaining CDD obligations.

It is known that early CDD measures can prevent receiving contaminated funds. Bravalla will apply a standard level of CDD measures before reaching the threshold above (NAf. 4,000), identifying the customer by collecting personal details (name, residential address, date of birth) and conducting sanctions screening, as follows:

Know your Customer (KYC) Procedure

When the customer creates their account on the platform, they will be asked for the following information, which must be filled in completely.

- CPF (National ID);

- Date of Birth;
- e-Mail;
- Phone Number;
- Address;
 - Street;
 - City;
 - State;

Identification data

All Customers must be brazilians and provide a CPF (Brazilian Tax identification number / Natural Persons register number).

As of January 11 2023, Brazilian federal law nº 14.534/23 was enacted considering the CPF to be unique and sufficient to identify citizens on government databases. The CPF is recorded on birth certificates & all identity documents.

What is checked using the CPF?

Four checks are made:

- 1) Does the CPF already exist within our system?
If yes, no new account is created. If not, the registration flow continues. This guarantees each account has a unique identifier and prevents duplicate accounts.
- 2) Is the CPF associated with someone over the age of 18?
If yes, registration flow continues. If not, no account will be created with this CPF.
- 3) Is the person alive or dead? (CPF also present on death certificates)
If dead, no account will be created with this CPF. If alive, registration can continue.
- 4) Does the CPF exist in the official individuals registry database of the country?
If yes, registration flow continues, if no, registration flow is stopped. A fake CPF cannot be used to register.

In order to verify that the identity provided corresponds to an individual legally identified according to the Curacao National Ordinance on Identification in Services (hereinafter



referred as to NOIS) and AML Regulation for Casinos, Bravalla uses the services provided by COMBATEAFRAUDE TECHNOLOGY OF INFORMATION S.A. (hereinafter CAF¹), a company registered under CNPJ/MF number 34.102.645/0001-57, with its headquarters at Rua Tiradentes, nº 1077 - 5th floor - Centro, Venâncio Aires - RS, BRAZIL ("CAF").

Within the framework of its operational protocols, Bravalla has established a contractual agreement with CAF (Customer Authentication Facility) to facilitate the seamless execution of identification data checks, ensuring compliance with pertinent regulations and standards. This agreement stipulates the automatic provision of relevant identity checks, thereby fostering a streamlined process in alignment with regulatory requirements.

As part of its commitment to operational excellence CAF's performance is verified through periodic testing procedures that take into account the geographical areas. These evaluations serve to validate the functionality and reliability of the authentication system, thereby upholding the integrity of Bravalla's operational infrastructure.

However, Bravalla acknowledges that notwithstanding the contractual arrangement with CAF and the latter's designated responsibilities, ultimate accountability for customer-centric risk assessments rests with the company itself. T

CAF provides a unified and effective solution for the identification and protection of our operation.

CAF provides services from registration to authentication. Bravalla has acquired the following services:

1. User onboarding
2. ID verification KYC
3. ID Document verification
4. Fraud prevention

¹ <https://www.caf.io/pt>



Upon including the CPF number in our platform, the ID verification KYC service is activated and CAF matches the information with the [Federal Revenue of Brazil record](#)². This tool provides information about the CPF registration status. Upon completing this step Bravalla has enough information in order to determine the customer identity. CAF processes are automatized with top technology. They also carry out operational security improvements in their flows constantly through a process called liveness by which they have a double check provided by their human resources.

Background checks are investigative processes used by Bravalla to verify and assess a person's history, particularly regarding their criminal record on ML/FT/FPWMD, and other relevant information. These checks are conducted to ensure safety and security.

Once the player has successfully registered their account, we immediately run a Sanctions background check using [Dilisense GmbH](#)³, a KYC provider based in Switzerland.

Bravalla sends the CPF details to Dilisense, who run that against their databases and return a match, a no match, or a potential match. Dilisense automatized tools review the sanction lists attached in annex A which include but are not limited to the UN and EU sanction list, U.S. Treasury's Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons List.

After concluding the automatized check the Dilisense platform informs Bravalla if there are findings or not.

While completing CDD measures, customers may continue using their gaming accounts. However, if the NAf. 4,000 threshold is reached, the player cannot deposit or withdraw funds until the necessary information is provided. If the required information is not received within 30 days after reaching the threshold, Bravalla will terminate the relationship and report the transaction to the FIU.

² <https://servicos.receita.fazenda.gov.br/servicos/cpf/consultasituacao/consultapublica.asp>

³ <https://dilisense.com/en>

Enhanced Due Diligence

A risk-based approach should be taken, with more thorough checks for higher-risk customers. Enhanced Due Diligence (EDD) measures should align with identified risks, increasing monitoring to detect unusual transactions or activities.

EDD is necessary for higher ML/TF risk scenarios, such as:

- Residents of higher-risk geographic areas
- Politically Exposed Persons (PEPs)
- Products or transactions favoring anonymity
- New products and business practices, including new technologies

EDD measures may include:

- Obtaining additional customer information (occupation, previous address, etc.)
- Understanding the intended nature of the business relationship
- Verifying the source of funds or wealth
- Approving the relationship at a senior management level
- Conducting enhanced monitoring
- Requiring the first payment through an account in the customer's name with a bank following similar CDD standards
- In higher-risk situations, source of funds information must be periodically requested even without changes in pattern or activity.

Politically Exposed Persons (PEPs)

Politically Exposed Persons (PEPs) are individuals who are or have been entrusted with a prominent public function by a government or an international organization. Given their status and authority, it is acknowledged that numerous PEPs occupy roles susceptible to exploitation for the perpetration of money laundering (ML) crimes and associated predicate offenses, such as corruption, bribery, and facilitation of terrorist financing (TF). This assertion finds validation through thorough analysis and documented case studies. When analyzing inherent risk and its factors particularly customers with this nature, it is

undeniable that threats linked to PEPs justify the implementation of supplementary AML/CFT/CFPWMD preventative measures concerning engagements with such individuals.

Recognizing this particular aspect within the Customers Factor as a compulsory prerequisite is precautionary rather than punitive in essence, and ought not to be misconstrued as casting suspicion on Politically Exposed Persons (PEPs) for engaging in illicit behavior. Please consider that declining to engage in a business affiliation with a PEP solely on the grounds of their status contravenes both the explicit language and underlying principles of Recommendation 12 of the Financial Action Task Force (FATF).

CAF and Dilisense facilitate the search for PEPs. Therefore, after conducting CDD the company will be able to identify whether the customer is a PEP or not.

Bravalla is required, in relation to foreign politically exposed persons (PEPs) (whether as customers or beneficial owners), to perform the following measures in addition to normal customer due diligence:

- a. Have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;
- b. Obtain senior management approval to service the PEP, whether for establishing a new business relationship, continuing an existing one, or conducting an occasional transaction.
- c. Take reasonable measures to establish the source of wealth and funds. The investigation should confirm whether the player's spending pattern matches their legal source of funds. This includes checking data bases with information about salary and credit score, requesting a statement from the player about the source of funds and verifying it using independent and reliable sources, starting with public sources and moving to documents provided by the customer if public sources are insufficient;
- d. Conduct enhanced ongoing monitoring of the business relationship.

Bravalla is required to determine if a customer is a domestic PEP or a person who has been entrusted with a prominent function by an international organization. In higher-risk

situations with such persons, Bravalla must apply the measures referred to in points b, c, and d.

Although stricter customer due diligence is required for each PEP, the measures are tailored to the specific risks associated with the PEP. Factors to consider include:

- The type of public function held by the PEP;
- The country of origin of the PEP;
- The transactions conducted by the PEP.
- These requirements also apply to family members or close associates of PEPs.

Screening for PEP status must be carried out before establishing the business relationship or conducting an occasional transaction, and regularly during the business relationship. If a player becomes a PEP after onboarding, Bravalla will implement the above measures within thirty days.

Application of CDD Measures to Existing Customers

On 20 May 2024, the Gaming Control Board (GCB) presented new regulations for Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation of weapons of mass destruction (AML/CFT/CFP Regulations) for the online gaming sector of Curacao. In order to execute the regulations, Bravalla should apply CDD measures to existing customers based on materiality and risk, conducting due diligence at appropriate times.

Termination of the Business Relationship

If customer due diligence obligations cannot be met, Bravalla cannot establish or must terminate the business relationship. Bravalla must keep records of all attempts to obtain the necessary information and documentation.

Bravalla may close the account or keep it blocked and suspended. If the customer provides the required information after closure or suspension, Bravalla will assess whether the delay affects the ML/FT risk. Bravalla must consider if there are grounds to suspect

ML/FT/FP and decide accordingly. When closing the accounts, funds should be returned to the player through the same channels used to receive them if there is no reason to retain them.

Reporting of Unusual Transactions

Reporting Obligations

Bravalla will detect and report unusual transactions, following procedures for recognizing, documenting, and reporting unusual transactions. An unusual transaction is one inconsistent with the player's profile. Bravalla will collect information to assess the risk associated with the player and build a customer profile.

Based on NORUT legislation, Bravalla will use objective and subjective indicators to assess if a transaction is unusual. The board of directors must provide the operations staff with guidance and training on recognizing and documenting unusual transactions.

Unusual transactions must be reported internally to the compliance officer, who maintains records. If not reported to the FIU, the reason must be documented and signed off by the compliance officer and/or board of directors.

Bravalla will pay special attention to complex, unusually large transactions, and unusual transaction patterns with no apparent economic or lawful purpose.

Examples of unusual transactions include:

- Transactions reported to the Police or Department of Justice for money laundering or terrorism financing;
- Transactions by entities named on a sanctions list;
- Transactions of NAf. 5,000 or more, whether cash, check, electronic, or other means.

Reporting Unusual Transactions



Under article 11 of the NORUT, casinos must report unusual or intended unusual transactions to the FIU without delay.

The Documentation of Unusual Transactions

Bravalla will register with the FIU and use the goAML reporting portal for external reporting. The compliance officer prepares reports of unusual transactions for the FIU, submitting them and related documents through the portal in English. Bravalla and its personnel are protected by law from liability when reporting to the FIU.

Prohibition of Disclosure

Bravalla and their staff must not disclose details of reports filed to the FIU or requests for information from the FIU to customers or third parties, to avoid compromising investigations. Drastic actions like terminating a relationship should only be taken when necessary to avoid alerting the player, with ongoing monitoring and additional reports to the FIU as preferable alternatives.

Record Keeping

Bravalla will maintain records of transactions for at least five years to comply with information requests from authorities. Records must be sufficient to reconstruct individual transactions for potential criminal prosecution. CDD records and business correspondence must be kept for five years after the business relationship ends or the occasional transaction date. CDD information and transaction records must be available to domestic authorities based on legal authority.



Annex A.

Africa African Development Bank
List name Debarred Entities # of records ~ 1.100 Link https://www.afdb.org Status Included Description The African Development Bank Group have imposed sanctions on entities found to have participated in fraudulent practices and are therefore ineligible to participate in contracts financed or administered by the African Development Bank Group.
Americas Inter-American Development Bank
List name Sanctioned Firms and Individuals # of records ~ 1.000 Link https://www.iadb.org Status Included Description The Inter-American Development Bank have sanctioned firms and individuals for engaging in fraudulent, corrupt, collusive, coercive or obstructive practices, in violation of the IDB Group's Sanctions Procedures and anti-corruption policies.
Asia Asian Development Bank
List name Sanction List

of records

~ 1.100

Link

<http://lnadbg4.adb.org>

Status

Included

Description

The Asian Development Bank have imposed sanctions on entities who violated the sanctions while ineligible; entities who committed second and subsequent violations; debarred entities who are uncontactable; and cross debarred entities

European Union

European Bank for R&D

List name

Sanctions from Debarment Decisions

of records

~ 900

Link

<https://www.ebrd.com>

Status

Included

Description

The European Bank for Reconstruction and Development have imposed sanctions on entities and individuals who are subject to Debarment Decision by a Mutual Enforcement Institution (e.g. African Development Bank, World Bank etc.).

European Union

European Bank for R&D

List name

EBRD-initiated and Third Party Sanctions

of records

~ 30

Link

<https://www.ebrd.com>

Status

Included

Description

The European Bank for Reconstruction and Development have imposed sanctions on entities and individuals who engaged in prohibited practices in the context of a bank project or are subject to a third party finding.

European Union

European Commission

List name

The EU Air Safety List

of records

~ 115

Link

<https://eeas.europa.eu>

Status

Included

Description

The EU Air Safety List actually contains two lists: The first list (Annex A) includes all airlines banned from operating in Europe. The second list (Annex B) includes airlines that are restricted from operating under certain conditions in Europe.

European Union

European Commission

List name

Consolidated List of Sanctions

of records

~ 2.200

Link

<https://eeas.europa.eu>

Status

Included

Description

Restrictive measures (sanctions) are an essential tool in the EU's common foreign and security policy (CFSP), through which the EU can intervene where necessary to prevent conflict or respond to emerging or current crises. The EU has over forty different sanctions regimes in place.

European Union

European Council

List name

European Council Regulation No 833/2014

of records

~ 20

Link

<https://eur-lex.europa.eu/homepage.html>

Status

Included

Description

The European Council defines the EU's overall political direction and priorities. The Council Regulation (EU) No 833/2014 of 31 July 2014 is concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.

European Union

European Council

List name

European Council Regulation 2022/398

of records

~ 5

Link

<https://eur-lex.europa.eu/homepage.html>

Status

Included

Description

Council Regulation (EU) 2022/398 of 9 March 2022 amending Regulation (EC) No 765/2006 concerning restrictive measures in view of the situation in Belarus and the involvement of Belarus in the Russian aggression against Ukraine.

European Union

European Council

List name

European Council Decision 2022/399

of records

~ 5

Link

<https://eur-lex.europa.eu/homepage.html>

Status

Included

Description

Council Decision (CFSP) 2022/399 of 9 March 2022 amending Decision 2012/642/CFSP concerning restrictive measures in view of the situation in Belarus and the involvement of Belarus in the Russian aggression against Ukraine.

United Nations

UN Security Council

List name

Consolidated List

of records

~ 1.000

Link

<https://www.un.org>

Status

Included

Description

The Consolidated List includes all individuals and entities subject to measures imposed by the Security Council. For each instance in response to a threat, a Security Council Committee manages the sanctions regime.

The World Bank

The World Bank

List name

Debarred Firms and Individuals

of records

~ 1.600

Link

<http://www.worldbank.org>

Status

Included

Description

The World Bank have imposed sanctions on firms and individuals meaning they are ineligible to be awarded a World Bank-financed contract for the periods indicated because they have been sanctioned under the Bank's fraud and corruption policy.

EMEA (Europe, Middle East and Africa)

Belgium

Federal Public Service Finance

List name
National Financial Sanctions
of records
~ 300
Link
<https://financien.belgium.be>
Status
Included
Description
The Belgian national list is adopted and modified by a Royal Decree adopted in implementation of the Royal Decree of December 28th 2006 as regards specific restrictive measures against some persons and entities within the framework of the fight against terrorism financing.

Bahrain
MOFA - Ministry of Foreign Affairs

List name
Bahrain Terrorist List
of records
~ 200
Link
<https://www.mofa.gov.bh>
Status
Included
Description
In 2005, the International Monetary Fund evaluated the procedures taken by the Kingdom of Bahrain to combat money laundering and terrorism financing. According to the resolutions issued after the evaluation, the Kingdom developed all the required legislation and practices.

Czech Republic
Ministry of Foreign Affairs

List name
National Sanctions List
of records
~ 5
Link
<https://www.mzv.cz/>
Status

Included

Description

According to Act No. 1/2023 Coll. on restrictive measures against certain serious acts applied in international relations, the Ministry of Foreign Affairs maintains a national sanctions list and publishes it on its website.

Egypt

Money Laundering Combating Unit

List name

Domestic Terrorist List

of records

~ 6.600

Link

<https://mlcu.org.eg>

Status

Included

Description

The Egyptian Money Laundering Combating Unit (EMLCU) was established under the Anti-Money Laundering Law promulgated by Law No. 80 of 2002, and is the Egyptian Financial Intelligence Unit that became operative in September 2002.

France

Ministère de l'Économie et des Finances

List name

Registre des Gels

of records

~ 2.400

Link

<https://www.tresor.economie.gouv.fr>

Status

Included

Description

Under Article L. 561-2 of the Monetary and Financial Code, persons subject to the AML/CFT regime are required to implement the asset freezes ordered by France. In order to enable professionals to meet these freezing obligations, a national register of persons and entities subject to a freezing measure is established.

Israel

Ministry of Defense - NBCTF

List name

Declarations On Activists

of records

~ 430

Link

<https://www.mod.gov.il>

Status

Included

Description

The National Bureau for Counter Terror Financing (NBCTF) issues this list in accordance with the Prohibition on Terrorist Financing Law 5765-2004 and the Counter Terrorism Law 2016. The NBCTF was established in March 2018 as a result of an Israeli Cabinet decision.

Israel

Ministry of Defense - NBCTF

List name

Unauthorized Assoc. & Terrorists Org.

of records

~ 420

Link

<https://www.mod.gov.il>

Status

Included

Description

The National Bureau for Counter Terror Financing (NBCTF) issues this list in accordance with the Defense Regulations (Emergency) 1945 and the Prohibition on Terrorist Financing Law 5765-2004 and the Prevention of Terrorism Ordinance No 33 5708-1948 and the Counter Terrorism Law 2016.

Lithuania

Financial Crime Investigation Service

List name

Tarptautinės Finansinės Sankcijos

of records

~ 15

Link

<https://www.fntt.lt>

Status

Included

Description

The goal of the Financial Crime Investigation Service is to elaborate methods of combating criminal activities against the State financial system.

Luxembourg

CSSF - Commission de Surveillance

List name

Sanction CSSF

of records

~ 100

Link

<https://www.cssf.lu>

Status

Included

Description

The Commission de Surveillance du Secteur Financier (CSSF) of Luxembourg conducts its prudential and market surveillance missions with the aim of contributing to the soundness and stability of the financial sector, exclusively in the public interest.

Netherlands

Government of the Netherlands

List name

Dutch National Sanction List Terrorism

of records

~ 40

Link

<https://www.government.nl>

Status

Included

Description

The Dutch national sanction list terrorism contains the names of individuals and organisations who are involved in terrorist activities. In accordance with UN Security Council Resolution 1373 (2001) their assets have been frozen.

Poland

Ministry of Affairs Interior and Administration

List name Sanction List # of records ~ 50 Link https://www.gov.pl/web/mswia Status Included Description Decisions of the Minister of Interior and Administration on entry on the list of persons and entities to whom the measures referred to in the Act on special solutions in the field of counteracting supporting aggression against Ukraine and serving to protect national security are applied.
Palestine Palestine Monetary Authority
List name Local Freezing List # of records ~ 5 Link http://www.pma.ps Status Included Description In line with authorities of the "Security Council Resolutions Enforcing Committee", which formed according to Decree No. (14) of 2015 Concerning the Enforcement of Security Council Resolutions, a Local Freezing List has been created.
Qatar Ministry of Interior
List name National Counter Terrorism List # of records ~ 800 Link https://portal.moi.gov.qa Status

Included

Description

The committee assumes its responsibilities in one of the most important security areas in order to ensure the achievement of the strategy of countries in the fight against terrorism through the security related efforts and cooperation with the relevant bodies.

South Africa

Financial Intelligence Centre (FIC)

List name

Targeted Financial Sanctions

of records

~ 540

Link

<https://www.fic.gov.za>

Status

Included

Description

The Financial Intelligence Centre (FIC) is the national centre for the receipt of financial data, analysis and dissemination of financial intelligence. The FIC was established by the FIC Act, 2001 (Act 38 of 2001) and has the mandate to identify the proceeds of crime, combat money laundering and terror financing.

Switzerland

State Secretariat for Economic Affairs

List name

Sanctions

of records

~ 2.000

Link

<https://www.seco.admin.ch>

Status

Included

Description

The State Secretariat for Economic Affairs have imposed sanctions based on the Federal Act on the Implementation of International Sanctions (Embargo Act, EmbA, 1st of January 2003). It has formed the legal basis for the implementation of sanctions imposed by Switzerland.

Ukraine

State Financial Monitoring Service

List name

Terrorist Activity List

of records

~ 1.000

Link

<https://fiu.gov.ua>

Status

Included

Description

The State Financial Monitoring Service of Ukraine (SFMS) is the national center for receiving and analyzing: suspicious transaction reports, information related to money laundering, terrorist financing and financing of the proliferation of weapons of mass destruction.

United Arab Emirates

CGMSIEC

List name

National Terrorist List

of records

~ 270

Link

<https://www.uaieic.gov.ae>

Status

Included

Description

In compliance with UN Security Council resolution No. 1730/2006 and pursuant to UAE Federal Law No. 7 of 2014, the UAE publishes the National Sanctions List containing the names of individuals and entities identified as terrorist and associated with proliferation of weapons of mass destruction.

United Kingdom

HMT - OFSI

List name

Financial Sanctions

of records

~ 2.300

Link

<https://www.gov.uk>

Status

Included

Description

The Office of Financial Sanctions Implementation (OFSI), part of Her Majesty's Treasury (HMT), have imposed sanctions to freeze assets, to prevent transit through their territories and to prevent the direct or indirect supply, sale and transfer of military equipment.

United Kingdom

HMT - OFSI

List name

Ukraine Restrictive Measures

of records

~ 10

Link

<https://www.gov.uk>

Status

Included

Description

List of persons subject to restrictive measures in view of Russia's actions destabilising the situation in Ukraine. These persons and certain other parties are subject to restrictive measures relating to transferable securities and money market instruments, as set out in Council Regulation (EU) No.833/2014.

United Kingdom

Foreign Secretary

List name

Corrupt Political Figures

of records

~ 30

Link

<https://www.gov.uk>

Status

Included

Description

The Foreign Secretary announced sanctions that target corrupt political figures, those violating human rights, and perpetrators of sexual-violence in conflict.

Americas (North, Central and South America)
Argentina RePET
List name Registro Público de Personas y Entidades # of records ~ 500 Link https://repet.jus.gob.ar Status Included Description The Argentine Ministry of Justice and Human Rights publishes a list of people and organizations related to terrorist attacks and their funding, also known as Registro Público de Personas y Entidades vinculadas a actos de Terrorismo y su Financiamiento.
Brazil Portal da Transparência do Governo Federal
List name Acordos de Leniência # of records ~ 100 Link https://www.portaltransparencia.gov.br Status Included Description Leniency Agreements
Brazil Portal da Transparência do Governo Federal
List name Empresas Inidôneas e Suspensas # of records ~ 15.600

Link

<https://www.portaltransparencia.gov.br>

Status

Included

Description

Disreputable and Suspended Companies

Brazil

Portal da Transparência do Governo Federal

List name

Entidades sem Fins Lucrativos Impedidas

of records

~ 4.000

Link

<https://www.portaltransparencia.gov.br>

Status

Included

Description

Prohibited Non-Profit Entities

Brazil

Portal da Transparência do Governo Federal

List name

Empresas Punidas

of records

~ 550

Link

<https://www.portaltransparencia.gov.br>

Status

Included

Description

Punished Companies

Canada

Department of Foreign Affairs and Trade

List name

Consolidated Autonomous Sanctions List

of records

~ 1.400

Link

<https://www.international.gc.ca>

Status

Included

Description

The Consolidated Canadian Autonomous Sanctions List includes individuals and entities subject to specific sanctions regulations made under the Special Economic Measures Act (SEMA) and the Justice for Victims of Corrupt Foreign Officials Act (JVCFOA).

Canada

Department of Justice

List name

Corrupt Foreign Nationals

of records

~ 70

Link

<https://laws-lois.justice.gc.ca>

Status

Included

Description

An individual whose name is listed in the schedule is a foreign national who, in the opinion of the Governor in Council, has committed an act set out in subsection 4(2) of the Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law).

Canada

Department of Justice

List name

Corrupt Foreign Officials (Tunisia)

of records

~ 10

Link

<https://laws-lois.justice.gc.ca>

Status

Included

Description

Tunisia and Egypt have asserted to the Government of Canada, in writing, that each of the persons listed has misappropriated property of Tunisia or of Egypt, as the case may be, or have acquired property inappropriately by virtue of their office or a personal or business relationship and have asked the Government of Canada to freeze the property of those persons.

Canada

Department of Justice

List name

Corrupt Foreign Officials (Ukraine)

of records

~ 15

Link

<https://laws-lois.justice.gc.ca>

Status

Included

Description

Ukraine has asserted to the Government of Canada, in writing, that each of the persons listed has misappropriated property of Ukraine or has acquired property inappropriately by virtue of their office or a personal or business relationship and Ukraine has asked the Government of Canada to freeze the property of those persons.

Canada

Department of Justice

List name

Regulations Establishing a List of Entities

of records

~ 80

Link

<https://laws-lois.justice.gc.ca>

Status

Included

Description

Her Excellency the Governor General in Council, on the recommendation of the Solicitor General of Canada, pursuant to subsection 83.05(1) of the Criminal Code, makes the annexed Regulations Establishing a List of Entities.

Canada

Department of Public Safety

List name

Canadian Counter-Terrorism Entity List

of records

~ 60

Link

<https://www.publicsafety.gc.ca>

Status

Included

Description

The listing of an entity is a public means of identifying a group or individual as being associated with terrorism. The definition of an entity includes a person, group, trust, partnership or fund, or an unincorporated association or organization.

USA

CBP - U.S. Customs and Border Protection

List name

North Korea Sanctions

of records

~ 230

Link

<https://www.cbp.gov>

Status

Included

Description

CBP and ICE, with the U.S. Department of State, and the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), issued the North Korea Sanctions and Enforcement Actions Advisory: Risks for Businesses with Supply Chain Links to North Korea on July 23, 2018.

USA

DDTC - Directorate of Defense Trade Controls

List name

AECA Debarred Statutory List

of records

~ 700

Link

<https://www.pmddtc.state.gov>

Status

Included

Description

The persons (including entities and individuals) have been convicted of violating or conspiracy to violate the Arms Export Control Act (AECA). They are subject to "statutory debarment" pursuant to §38(g)(4) of the AECA and §127.7 of the International Traffic in Arms Regulations (ITAR).

USA

DDTC - Directorate of Defense Trade Controls

List name

AECA Debarred Administrative List

of records

~ 5

Link

<https://www.pmddtc.state.gov>

Status

Included

Description

The U.S. Department of State - Directorate of Defense Trade Controls (DDTC) may impose administrative debarment for violations of the Arms Export Control Act (AECA/ITAR), as specified in 22 CFR §127.7(a), upon resolution of enforcement proceedings.

USA

DOS - Department of State

List name

Nonproliferation Sanctions

of records

~ 600

Link

<https://www.state.gov>

Status

Included

Description

The U.S. Department of State have imposed sanctions under various legal authorities against foreign individuals, private entities, and governments that engage in proliferation activities. The Federal Register notices are the official notifications for all nonproliferation sanctions determinations.

USA

DOS - Department of State

List name

Cuba Restricted List

of records

~ 240

Link

<https://www.state.gov>

Status

Included

Description

The U.S. Department of State's list of entities and subentities under the control of, or acting for or on behalf of, the Cuban military, intelligence, or security services or personnel with which direct financial transactions would disproportionately benefit such services or personnel at the expense of the Cuban people or private enterprise in Cuba.

USA

DOS - Department of State

List name

Section 7031(c)

of records

~ 350

Link

<https://www.state.gov>

Status

Included

Description

Section 7031(c) of the Department of State, Foreign Operations, and Related Programs Appropriations Act, Congress provides that officials of foreign governments and their immediate family members are ineligible for entry into the United States when the Secretary of State has credible information that the foreign official has been involved, directly or indirectly, with significant corruption and/or a gross violation of human rights.

USA

DOS - Department of State

List name

Terrorist Exclusion List

of records

~ 60

Link

<https://www.state.gov>

Status

Included

Description

Section 411 of the USA PATRIOT ACT of 2001 (8 U.S.C. § 1182) authorized the Secretary of State, in consultation with or upon the request of the Attorney General, to designate terrorist organizations for immigration purposes. This authority is known as the "Terrorist Exclusion List (TEL)" authority.

USA

OFAC - Department of Treasury

List name

Non-SDN sanction list

of records

~ 400

Link

<https://www.treasury.gov>

Status

Included

Description

The U.S. Office of Foreign Asset Control (OFAC) have imposed sanctions on non-specially designated nationals (SDN) which were consolidated from the FSE list, the SSI list, the NS-PLC list, the list of Foreign Financial Institutions Subject to Part 561, the non-SDN Iranian Sanctions Act list and the list of Foreign Financial Institutions Subject to the CAPTA List.

USA

OFAC - Department of Treasury

List name

Specially Designated Nationals

of records

~ 8.500

Link

<https://www.treasury.gov>

Status

Included

Description

The U.S. Office of Foreign Asset Control (OFAC) publishes lists of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities designated under programs that are not country-specific. Collectively, such individuals and companies are called 'Specially Designated Nationals' (SDNs).

USA

OFAC - Department of Treasury

List name

Executive Order 13959 of Nov. 12, 2020

of records

~ 30

Link

<https://www.treasury.gov>

Status

Included

Description

The President of the United States manages the operations of the Executive branch of Government through Executive Orders. The Executive Order 13959 of November 12, 2020 is addressing the threat from securities investments that finance communist Chinese military companies.

USA

OFAC - Department of Treasury

List name

31 CFR part 587 - General License 26

of records

2

Link

<https://www.treasury.gov>

Status

Included

Description

OFAC is issuing the Russian Harmful Foreign Activities Sanctions Regulations, 31 CFR part 587, to implement E.O. 14024, pursuant to authorities delegated to the Secretary of the Treasury in E.O. 14024.

USA

OFAC - Department of Treasury
List name 31 CFR part 587 - General License 30 # of records 1 Link https://www.treasury.gov Status Included Description OFAC is issuing the Russian Harmful Foreign Activities Sanctions Regulations, 31 CFR part 587, to implement E.O. 14024, pursuant to authorities delegated to the Secretary of the Treasury in E.O. 14024.
USA OFAC - Department of Treasury
List name 31 CFR part 587 # of records 15 Link https://www.treasury.gov Status Included Description OFAC is issuing the Russian Harmful Foreign Activities Sanctions Regulations, 31 CFR part 587, to implement E.O. 14024, pursuant to authorities delegated to the Secretary of the Treasury in E.O. 14024.
USA BIS - Bureau of Industry and Security
List name Denied Persons List # of records ~ 600 Link https://www.bis.doc.gov Status

Included

Description

The U.S. Bureau of Industry and Security imposed sanctions on persons who violated against the U.S. export law and for which the export privileges have been denied by written order of the Department of Commerce. Each order affecting export privileges is published in the Federal Register.

USA

BIS - Bureau of Industry and Security

List name

Entity List

of records

~ 1.500

Link

<https://www.bis.doc.gov>

Status

Included

Description

The U.S. Export Administration Regulations (EAR) contain a list of names of certain foreign persons – including businesses, research institutions, government and private organizations, individuals, and other types of legal persons – that are subject to specific license requirements for the export, reexport and/or transfer (in-country) of specified items.

USA

BIS - Bureau of Industry and Security

List name

Unverified list

of records

~ 150

Link

<https://www.bis.doc.gov>

Status

Included

Description

Parties listed on the Unverified List (UVL) are ineligible to receive items subject to the Export Administration Regulations (EAR) by means of a license exception. Restrictions on exports, reexports and transfers (in-country) to persons listed on the

UVL are set forth in Section 744.15 of the EAR. The Unverified List is set forth in Supplement No. 6 to Part 744 of the EAR.

USA

BIS - Bureau of Industry and Security

List name

Military End User (MEU) List

of records

~ 110

Link

<https://www.bis.doc.gov>

Status

Included

Description

The Military End User List identifies foreign parties that are prohibited from receiving items described in Supplement No. 2 of Part 744 of the EAR unless the exporter secures a license. These parties have been determined by the U.S. Government to be 'military end users,' and represent an unacceptable risk of use in China, Russia, or Venezuela.

USA

DOD - Department of Defense

List name

Section 1237

of records

~ 10

Link

<https://www.defense.gov>

Status

Excluded

Description

As of June 3, 2021, the Secretary of Defense has removed the entities listed from the CCMC list.

USA

DOD - Department of Defense

List name

Section 1260H

of records

~ 50

Link

<https://www.defense.gov>

Status

Included

Description

The Department of Defense released the names of “Chinese military companies” operating directly or indirectly in the United States in accordance with the statutory requirement of Section 1260H of the National Defense Authorization Act for Fiscal Year 2021.

USA

Office of the Comptroller of the Currency

List name

Enforcement Actions

of records

~ 9.700

Link

<https://apps.occ.gov>

Status

Included

Description

The U.S. Office of the Comptroller (OCC) supervises the following entities and has the statutory authority to take enforcement actions against them: National banks and their subsidiaries, Federally chartered savings associations and their subsidiaries, Federal branches and agencies of foreign banks, Institution-affiliated parties (IAPs).

APAC (Asia-Pacific)

Australia

Department of Foreign Affairs and Trade

List name

Consolidated List

of records

~ 1.800

Link

<https://dfat.gov.au>

Status

Included

Description

The Department of Foreign Affairs and Trade of Australia (DFAT) have imposed financial sanctions and travel bans on persons and entities to which the Charter of the United Nations Act 1945 and the Autonomous Sanctions Act 2011 currently applies.

Azerbaijan

Financial Monitoring Service

List name

Domestic Sanction List

of records

~ 200

Link

<http://www.fiu.az>

Status

Included

Description

Domestic List of natural and legal persons subject to sanctions based on legislation of and international instruments, which the Republic of Azerbaijan is a party to, as well as relevant resolutions of the United Nations Security Council.

Bangladesh

Bangladesh Financial Intelligence Unit

List name

Sanction List

of records

~ 10

Link

<https://www.bb.org.bd>

Status

Included

Description

Bangladesh Financial Intelligence Unit (BFIU) is the central agency of Bangladesh responsible for analyzing Suspicious Transaction Reports (STRs), Cash Transaction Reports (CTRs) & information related to money laundering (ML) /financing of terrorism (TF) received from reporting agencies & other sources.

China

China Securities Regulatory Commission

List name

Administrative Penalties and Enforcements

of records

~ 1.500

Link

<http://www.csrc.gov.cn>

Status

Included

Description

China Securities Regulatory Commission (CSRC), a ministerial-level public institution directly under the State Council, performs a unified regulatory function, according to the relevant laws and regulations, and with the authority by the State Council.

India

Ministry of Home Affairs

List name

Banned Organizations

of records

~ 60

Link

<https://www.mha.gov.in>

Status

Included

Description

The source from the Ministry of Home Affairs (MHA) contains terrorist organisations listed in the first schedule of the unlawful activities (prevention) act, 1967 and unlawful associations under section 3 of unlawful activities (prevention) act, 1967.

Indonesia

Financial Transaction Reports Center

List name

DTTOT & Proliferasi WMD

of records

~ 520

Link

<http://www.ppatk.go.id>

Status

Included

Description

The Financial Transaction Reports and Analysis Center (PPATK) is a central institution that coordinates the implementation of efforts to prevent and eradicate money laundering in Indonesia. PPATK has the duty and authority to receive financial transaction reports, conduct analysis of financial transaction reports, and forward the results of the analysis to law enforcement agencies.

Japan

Ministry of Finance

List name

Asset Freeze List

of records

~ 2.200

Link

<https://www.mof.go.jp>

Status

Included

Description

Asset freezes based on the Foreign Exchange Act.

Japan

METI - Ministry of Economy

List name

Trade and Industry End User List

of records

~ 530

Link

<https://www.meti.go.jp>

Status

Included

Description

The Ministry of Economy, Trade and Industry (METI) has issued the End User List, providing exporters with information on foreign entities for which concern cannot be eliminated regarding involvement in activities such as the development of weapons of mass destruction (WMDs) and other items.

Kyrgyzstan

FIU - Financial Intelligence Unit

List name

Consolidated Sanctions List

of records

~ 1.000

Link

<https://fiu.gov.kg>

Status

Included

Description

The Financial Intelligence Unit (FIU) of the Kyrgyz Republic was established with the beginning of membership in the Eurasian Regional Group (EAG). The FIU is responsible, inter alia, for implementing decisions in the field of combating money laundering and the financing of terrorism.

Malaysia

Ministry of Home Affairs

List name

Sanction List

of records

~ 60

Link

<http://www.moha.gov.my>

Status

Included

Description

This list is made by the Minister of Home Affairs under the section 66B (1) of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds From Illegal Activities 2001 [Act 613]. Under section 66B (1) of the Act 613, Where the Minister of Home Affairs is satisfied on information given to him by a police officer.

New Zealand

New Zealand Police

List name

Resolutions 1267/1989/2253/1988/1373

of records

~ 500

Link

<http://www.police.govt.nz>

Status

Included

Description

The UNSC 1267/1989/2253 and 1988 Committees specifically obliges New Zealand to take action against those terrorist entities it lists. UNSC Resolution 1373 obliges New Zealand (among other things) to outlaw the financing of, participation in and recruitment to, terrorist entities.

New Zealand

New Zealand Foreign Affairs & Trade

List name

Russian Sanctions

of records

~ 1.000

Link

<https://www.mfat.govt.nz>

Status

Included

Description

The Russia Sanctions Act 2022, passed unanimously by Parliament on 9 March 2022, is Aotearoa New Zealand's response to Russia's illegal and unprovoked invasion of Ukraine.

Pakistan

National Counter Terrorism Authority

List name

Proscribed Organizations

of records

~ 80

Link

<https://nacta.gov.pk>

Status

Included

Description

The Government of Pakistan with its National Counter Terrorism Authority (NACTA) under section 11-B of Anti Terrorism Act can declare an organization believed to be concerned with terrorism as a Proscribed Organization or put it under surveillance.

Pakistan

National Counter Terrorism Authority
List name Proscribed Persons # of records ~ 3.200 Link https://nacta.gov.pk Status Included Description Any individual about whom either there is a credible intelligence-information or who has a history of being linked to a Proscribed Organization can be proscribed by Home Department of a Province and can be subjected to restrictions on travel, speech and business, under the Anti Terrorism Act, 1997.
Singapore Singapore Statutes Online
List name Terrorism (Suppression of Financing) Act # of records ~ 40 Link https://sso.agc.gov.sg Status Included Description The Singaporean Government have imposed sanctions to suppress the financing of terrorism, to give effect to the International Convention for the Suppression of the Financing of Terrorism and for matters connected therewith.
Thailand Anti-Money Laundering Office
List name Designated List # of records ~ 180 Link https://www.amlo.go.th

Status

Included

Description

The Anti-Money Laundering Office (AMLO) of Thailand is a government agency, not under Prime Minister's Office or any Ministry. The office works independently and is answerable to the Prime Minister. It is mandated under Section 40 of the Anti-Money Laundering Act, 1999 and its amendments.

Dilisense automatized tools additionally checks the following criminal background on a global scale for Bravalla.

Criminal background checks on a global scale

United Arab Emirates

Dubai Financial Services Authority

List name

Register of Restricted Individuals

of records

~ 20

Link

<https://www.dfsa.ae>

Status

Included

Description

In addition to regulating financial and ancillary services, the DFSA is responsible for supervising and enforcing anti-money laundering (AML) and counter-terrorist financing (CTF) requirements applicable in the DIFC.

Canada

RCMP

List name

Wanted Persons

of records

~ 90

Link

<https://www.rcmp-grc.gc.ca>

Status

Included

Description

At the community, provincial, territorial and federal levels, Royal Canadian Mounted Police (RCMP) work to prevent crime, enforce the law, investigate offences, keep Canadians, and their interests, safe and secure, assist Canadians in emergency situations/incidents.

Canada

BC RCMP

List name

Wanted Persons

of records

~ 60

Link

<https://bc-cb.rcmp-grc.gc.ca>

Status

Included

Description

The British Columbia Royal Canadian Mounted Police (BC RCMP) proudly provides municipal, provincial and federal policing in areas that range from isolated Aboriginal communities and coastal villages to major cities.

Germany

Bundeskriminalamt

List name

Fahndungen

of records

~ 20

Link

<https://www.bka.de>

Status

Included

Description

The Bundeskriminalamt is an essential cornerstone in a comprehensive system of crime control and works as a partner with the police forces of the Federation and of the individual German states.

European Union

Europol

List name

Europe's Most Wanted Fugitives

of records

~ 40

Link

<https://eumostwanted.eu>

Status

Included

Description

Headquartered in The Hague, the Netherlands, Europol support the 27 EU Member States in their fight against terrorism, cybercrime and other serious and organised forms of crime. Europol also work with many non-EU partner states and international organisations.

Ghana

Ghana Police Service

List name

Wanted Persons

of records

~ 5

Link

<https://police.gov.gh>

Status

Included

Description

The Ghana Police Service exists to deliver services in Crime Prevention Detection, Apprehension and Prosecution of offenders consistent with the expectations of Ghana stakeholders for Maximum Protection, Safe, Secure and Peaceful Communities.

Hong Kong

Hong Kong Police Force

List name

Wanted Persons with Reward Notices

of records

~ 10

Link

<https://www.police.gov.hk/index.html>

Status

Included

Description

The vision is to maintain Hong Kong as one of the safest and most stable societies in the world. In this fast-changing world, emerging crime trends, global terrorism threats and unprecedented disasters have remained relevant in the global context.

International

Interpol

List name

Interpol Most Wanted List

of records

~ 7.300

Link

<https://www.interpol.int>

Status

Included

Description

The Interpol Most Wanted List contains fugitives wanted either for prosecution or to serve a sentence. Law enforcement worldwide is requested to locate and provisionally arrest a person pending extradition, surrender, or similar legal action.

Lithuania

IRD - VRM

List name

Suspects, Accused & Convicts

of records

~ 10.000

Link

<https://www.ird.lt>

Status

Included

Description

The Register of Suspects, Accused and Convicts was set up in 2012 by the Information Technology and Communications Department (IRD) under the Ministry of

the Interior (VRM) of the Republic of Lithuania which is the administrator of the register.

USA

ATF

List name

Most Wanted

of records

~ 10

Link

<https://www.atf.gov>

Status

Included

Description

The Bureau of Alcohol, Tobacco, Firearms and Explosives protects the public from crimes involving firearms, explosives, arson, and the diversion of alcohol and tobacco products; regulates lawful commerce in firearms and explosives.

USA

Federal Bureau of Investigation

List name

Most Wanted List

of records

~ 960

Link

<https://www.fbi.gov>

Status

Included

Description

The FBI is an intelligence-driven and threat-focused national security organization with both intelligence and law enforcement responsibilities. The FBI Most Wanted List includes the ten most wanted persons, fugitives, terrorists, parental kidnapers and bank robbers.

USA

Drug Enforcement Administration

List name

Most Wanted List

of records

~ 700

Link

<https://www.dea.gov>

Status

Included

Description

The DEA enforce the controlled substances laws and regulations of the United States. The DEA Most Wanted List includes fugitives involved in the growing, manufacture, or distribution of controlled substances appearing in or destined for illicit traffic in the US.

USA

US Marshals Service

List name

Fugitives

of records

~ 410

Link

<https://www.usmarshals.gov>

Status

Included

Description

The United States Marshals Service (USMS) is the nation's first and most versatile federal law enforcement agency, involved in virtually every federal law enforcement initiative. Its mission is to protect, defend, and enforce the American justice system.



This handbook and the information contained herein is the property of Bravalla Serviços de Gestão de Marcas and KTO Group Any reproduction of its content is prohibited except as authorized in writing by KTO Group.

Version 4 updated to 28 April 2024.