AML / CTF Program and Policy

Version: 2021.03-02

Arf Labs OÜ | www.arf.one

Registration Nr: 14715754

Harju maakond, Tallinn, Lasnamäe linnaosa, Lasnamäe tn 4b-26, 11412, Estonia

TABLE OF CONTENTS

1 VERSION AND AUTHORIZATION

Version	Explanation of changes/updates	Date of Updates	Effective Date Of Implementation
2021/03 -02	**Addition of UAB "PAYRNET specific processes**	**March 2021**	**March 2021**

Senior Management Acknowledgement of Changes– Reviewed and Approved by:			
Senior Management Name:	Berhan Kongel		
Senior Manager Title:	CEO	Date of Approval:	
Senior Manager Signature:			

Refer to Appendix A for the revision history for previous AML/CTF Policy documentation.

2 BACKGROUND

4AMLD was agreed by the EU in 2015 and required transposition into national laws by June 2017. Following its predecessors, it again followed the precedent set by FATF, drawing upon its refreshed Recommendations from 2012, which provided more detailed guidance on taking a risk-based approach (RBA) in the implementation of CDD.

As with previous directives, it also continued to widen the scope of AML/CFT obligations, including many exceptions from the financial and DNFBP sectors that had previously escaped inclusion, such as all gambling-based firms. Certain 'occasional transactions' over €10,000 outside of a business relationship also became subject to AML regulation, although member states found this a difficult requirement to implement.

In addition to this widening of scope, 4AMLD put a new emphasis on creating more transparency around structures launderers could use to hide the proceeds of bribery, corruption and tax evasion – crimes that were generating increasing media interest in the wake of the GFC. The directive thus included the requirement that Ultimate Beneficial Owners (UBOs), determined as those who owned 25% or more of a legal entity, appear on national registries, produced and maintained by member states' competent authorities, in order to reduce the opacity of corporate structures behind which some financial criminals had hidden.

The directive also looked at Enhanced Due Diligence for Politically Exposed Persons (PEPs), while expanding the scope of the term to include not only foreign nationals but domestic politically linked individuals as well.

Just over a year later – a record turnaround time for the EU – the fifth Anti Money Laundering Directive (5AMLD) came into force on 9 July 2018, requiring transposition by 10 January 2020. CFT concerns shaped much of the content and framing of the directive, as Europe faced a succession of Islamic State-inspired terrorist attacks, from the Bataclan and Charlie Hebdo attacks in Paris in 2015, through to the London Bridge attack in June 2017. Such was the psychological impact of these attacks on the EU, the Commission began drafting 5AMLD before it had even implemented its predecessor – an unprecedented action.

A prominent element of the directive was directed at reducing the financial options that had been used by the attackers to help conduct their attacks. The most prominent change in this regard was

the reduction in prepaid card limits, a product that had played a significant role in the preparation for the Bataclan attack.

Moreover, the directive added further detail to its 'transparency agenda,' requiring that national UBO registers go public in March 2020 and creating national functional PEP lists to identify the roles which qualified as 'PEPs' (and by exclusion, those which did not). However, as with previous directives, the process of implementation in some jurisdictions has proved bumpier than in others, perhaps not helped by the arrival of the COVID-19 pandemic early in the year.

Now the 6AMLD is on its way which aims to strengthen regulation and sanctions over the money laundering and terrorist financing infringements.

3 ARF AS DISTRIBUTOR OF UAB "PAYRNET"

Arf Labs OÜ ("**Arf**" or the "**Company**") is operating as an appointed distributor of UAB "PAYRNET", which is incorporated in Lithuania and authorised as an Electronic Money Institution in Lithuania and to this extent Arf must also follow and apply certain Lithuanian legal requirements, including those deriving from Lithuanian Law on the Prevention of Money Laundering and Terrorist Financing.

Due to distributor's status, Arf and its activities should be supervised and monitored by UAB "PAYRNET". This is required based on legal requirements applicable to UAB "PAYRNET" the aim of which is to ensure the proper and compliant provision of licensed services through selected distribution channels (including appointed distributors) since from the regulatory point of view UAB "PAYRNET" shall remain ultimately responsible for the compliance and legitimacy of appointed distributor's actions in relation to provision of such services on behalf of UAB "PAYRNET". Considering this, certain supervision and control measures might be applied by UAB "PAYRNET" over the Company as distributor, including the following ones (the list should not be considered as exhaustive):

- Chief Compliance Officer of Arf shall be assigned to be responsible for the communication with UAB "PAYRNET" and shall collect information on Arf's, as distributor's of UAB "PAYRNET", activity, including number of clients serviced by Arf as an appointed distributor of UAB "PAYRNET" during the reporting time slot, profiles of such clients (e.g. types of clients, from what jurisdictions they are, to which risk groups they were assigned, number of clients

with whom business relationship were terminated, etc.) in order to be able to report to UAB "PAYRNET", if so requested;

- Management of UAB "PAYRNET" will always have a right to request information and / or documents related to activities of Arf, as UAB "PAYRNET"'s distributor;
- UAB "PAYRNET" will have a right to execute internal audit covering assessment of Company's activities and their compliance with applicable AML / CTF requirements (to the extent related to Company's services provided in its status as a distributor of UAB "PAYRNET");
- UAB "PAYRNET" will have a right to perform ad hoc audits over activities of Arf (to the extent related to its status as distributor of UAB "PAYRNET"). For instance, to check few customers' files aiming to understand whether the Company complies with the legal requirements;
- UAB "PAYRNET" will acquaint the Company with its own AML / CTF procedures and all subsequent changes. The Company must ensure proper implementation of UAB "PAYRNET"'s requirements in the AML / CTF area.

As from a regulatory point of view UAB "PAYRNET" remains ultimately responsible for the provision of licensed services through Arf as distributor of UAB "PAYRNET", it is crucial for UAB "PAYRNET" to ensure that activities of the Company are in line with applicable requirements. For this purpose, UAB "PAYRNET" will share its own AML / CTF Policy with Arf prior to Arf starts providing services to clients as a distributor of UAB "PAYRNET". The Company will have a duty to review the UAB "PAYRNET"'s AML / CTF Policy and tailor its own AML / CTF procedures so that they would be compliant with the ones applied by UAB "PAYRNET". As both AML Policies (of UAB "PAYRNET" and the Company) are prepared inter alia based on Lithuanian legal requirements, they should match and not contradict each other in key areas.

4 DEFINITIONS

The following are a list of abbreviations and definitions used throughout this document:

AML	Anti-Money Laundering
CTF	Counter Terrorist Financing
EDD	Enhanced Due Diligence

New Technologies	New technologies refer to new products, services or delivery channels (e.g. mobile payment application), as well as internal systems that Arf Labs OÜ. uses to mitigate its inherent money laundering and terrorist financing risk, including, but not limited to, systems for client identification, sanction screening and transaction monitoring.
Money laundering ("ML")	Knowingly or recklessly dealing with the proceeds or property derived directly or indirectly as a consequence of an indictable offence, with the intent to conceal or convert any part of them. Concealment is a not necessary for an offence and conversion can be as simple as a deposit or a transfer.
Proceeds	Proceeds refers to any property derived from or obtained, directly or indirectly, through the commission of an offence.
Terrorism financing ("TF")	Terrorist financing is the financing of terrorist acts, and of terrorists and terrorist organisations.
Terrorist	The term terrorist refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts ; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Terrorist Act	A terrorist act includes: a) an act which constitutes an offence within the scope of, and as defined in one of the following treaties: (i) Convention for the Suppression of Unlawful Seizure of Aircraft (1970); (ii) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971); (iii) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973); (iv) International Convention against the Taking of Hostages (1979); (v) Convention on the Physical Protection of Nuclear Material (1980); (vi) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988); (vii) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (2005); (viii) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (2005); (ix) International Convention for the Suppression of Terrorist Bombings (1997); and (x) International Convention for the Suppression of the Financing of Terrorism (1999). b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.
Terrorist Organisation	The term terrorist organisation refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates

	as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Transaction Volume	References in this document to transaction volume, describe the total dollar value associated with a transaction or series of transactions.

5 INTRODUCTION

Arf operates as a technology service provider that is built on top of the infrastructures of regulated financial institutions. Arf's API stitches together the necessary parts of the underlying financial and compliance infrastructures to offer digital, seamless and instant global payment rails and value-add services to its customers.

Arf's cutting-edge payment rails technology coupled with its easy-to-deploy API enables instant international payouts for companies of the 21st century.

Arf's primary customer segments include gig-economy companies and online marketplaces in the EEA that need to make non-regular payouts to their customers and vendors inside and outside of the EEA. Arf's initial target segment is gig-economy companies in the EEA. The specific sub-segment Arf is going after is professional service companies which are on-demand platforms for sourcing business-related services and other high-skilled services. This is a $6B a year market in disbursement volume that is projected to grow to $13.4B by 2023.

It is incumbent on the Company to ensure it effectively identifies and mitigates the risks that may exist in its customer base, products and services offered, transactions and in the geographic areas in which it operates and/or transacts. This AML/CTF Policy is a crucial step towards achieving that goal.

6 RATIONALE AND OBJECTIVES

In order to develop a robust, and comprehensive anti-money laundering and counter-terrorist financing ("AML/CTF") compliance program, and pursuant to the requirements specified by the Legislation, Arf has prepared an AML/CTF Policy. The policy is designed to prohibit and actively prevent money laundering and financing of terrorism and crime and any activity that facilitates such acts. This document is created and maintained by Arf's Chief Compliance Officer ("CCO").

7 CHIEF COMPLIANCE OFFICER

Arf's board of directors/senior management appoints a Chief Compliance Officer and ensures that this position remains filled at all times by an individual with sufficient knowledge and experience to identify relevant risks, as well as a comprehensive understanding of Arf's regulatory obligations.

The CCO has responsibility for Arf's AML/CTF activities, monitoring the compliance programme including but not limited to:

- Identify any situations of higher risk of money laundering or terrorist financing;
- Maintain a record of its policies, controls and procedures, risk assessment and risk management including the application of such policies and procedures;
- Apply measures to ensure that its policies, controls and procedures are taken into account in all relevant functions including in the development of new products, dealing with new customers and in changes to business activities; and
- Provide information to Company's senior management and to UAB "PAYRNET" about the operation and effectiveness of its policies, controls and procedures whenever appropriate and at least annually.

- Ensure proper and timely communication with UAB "PAYRNET", reporting suspicious activity reports to the MLRO of UAB "PAYRNET", providing information requested by UAB "PAYRNET", ensuring that UAB "PAYRNET"'s requirements towards the implementation of ML / TF prevention are properly ensured and implemented, etc.

8 RISK BASED APPROACH

8.1 SUMMARY

The Company has adopted a Risk Based Approach ("RBA") for identifying, assessing, understanding, and mitigating the ML/TF risks to which Arf is exposed. The RBA is important for analysing the threats and vulnerabilities to ML/TF that puts the integrity of both the Company and the European financial system at risk. The RBA also helps Arf to assess the level of risk associated with various factors and to develop appropriate controls and strategies to mitigate these risks.

ML risks are risks associated with the introduction of proceeds of crime into the Company's transaction flow. TF risks are the risks associated with the introduction of property, which is owned

or controlled, directly or indirectly by a terrorist group, or intended to support terrorist causes, into the Company's transaction flow. ML/TF risks are assessed based on:

- Arf's products, services, and delivery channels;
- The geographies which are relevant to the Company; and
- The characteristics, activities, and transaction patterns of the Company's clients.

The RBA includes the following steps:

- Establishing a risk tolerance/appetite which articulates the maximum residual ML/TF risk that Arf is willing to accept;
- Identifying and assessing the inherent risks related to products, services, and access channels, geographical location, business relationships, new technologies, affiliates, and other relevant factors;
- Mitigating identified inherent risks by mapping, developing, and implementing effective controls;
- Reviewing the RBA at least once per 18-month period to evaluate its effectiveness at assessing ML/TF risks, the effectiveness of the controls at mitigating the assessed risks and revisiting whether the residual risk of any of the Company's activities exceeds the Company's risk tolerance; and
- Reporting activities, which exceed Arf's risk tolerance to senior management and the board of directors (the "**Board**"), along with details about the effectiveness of the respective controls.

Details about the RBA can be found on the following document: **Arf (AML-CTF) Risk Assessment and Risk Based Approach Methodology ("RBA Document").** Below are the key points of Arf's risk-based approach.

8.2 RISK TOLERANCE

The Company has established quantifiable thresholds using key risk indicators, which have been approved by Arf's board of directors (the "**Board**"). A breach of any of these indicators must be reported to the Board immediately. Arf has additionally established warning thresholds that allow management to take corrective actions to prevent a breach of the risk tolerance thresholds.

Further, the Company has defined certain jurisdictions and entity types that are outside of Arf's tolerance of risk. Conducting transactions involving these jurisdictions or entity types is prohibited without the express permission of the CCO.

8.3 DELIVERY CHANNELS

The Company assigns an inherent risk rating of low, medium or high to each delivery channel based on the security of connection that is offered by that channel. Arf has assessed the following inherent risk ratings to its delivery channels:

- Arf Dashboard – Medium risk
- Arf API – Low risk

8.4 GEOGRAPHIC RISK

The Company has assessed the risk that stems from the jurisdictions where the Company is located, as well as the jurisdictions to which the Company sends payments or from which Arf receives payments, using the methodology defined by KnowYourCountry. Each country is assigned a rating of low, low-medium, medium, medium-high, or high.

Countries that have been targeted by sanctions issued by either the EU, UNO or the US are restricted. See Appendix B for details about high-risk, prohibited and sanctioned countries.

8.5 PRODUCT AND SERVICE RISK

The inherent risk of the Company's products and services is determined by the risk of:

- the inherent risk of the delivery channels that are used to access the products and services;
- the inherent risk of the jurisdictions that are involved in the transactions that are conducted using the products and services; and
- the risk of the clients that use Arf's products and services.

8.6 TRANSACTION RISK

Arf has developed a methodology for identifying those transaction types that represent a higher level of money laundering and terrorist financing, with consideration of:

- The risk of the product or service that is being utilized;
- The geography risk of the jurisdiction or currency that is involved in the transaction;
- The value of the transaction; and

- The risk of the client that is conducting the transaction.

For transactions that are deemed to represent a higher level of risk, the Company conducts enhanced due diligence. Specifically, when conducting a high-risk transaction, Arf requires clients to provide documentation supporting the purpose of the transaction, such as an invoice. Exemptions from this obligation can be granted by the CCO or delegate.

8.7 RELATIONSHIP RISK

The Company assigns an inherent risk rating of low or high to each of its clients based on the following factors:

- Client Geography
- Length of Transaction History
- Transactional Activity
- Client Industry

There are also single high-risk factors that are taken into consideration while assigning the risk rating such as a Suspicious Activity Report submitted for a client in the past 24 months or a PEP is found to be associated with the client.

The Company conducts an Enhanced Due Diligence for high-risk clients which includes requesting additional documentation and more scrutiny over the transaction flow of the client. Details about prohibited and high-risk industries can be found in Appendix C.

8.7.1 CLIENT RISK ASSESSMENT METHODOLOGY

When conducting a risk assessment for a client the Company considers numerous factors, including the client's product and service utilization, residential location, the number of transactions that the client has conducted, certain transactional activity and client industry.

Company has weighted risk factors based on the magnitude of risk that the Company has determined is associated with each factor. Single high-risk factors are assigned six points, which is the maximum weighting, to ensure that the presence of those factors automatically result in a client being rated as high-risk.

Company uses the *Client Risk Assessment* form in Appendix D of the RBA Document to determine and monitor the risk ratings for clients that are in a business relationship.

Clients that fit the following profile are automatically deemed to be high risk independent of the Client Risk Assessment:

- Individuals (or in the case of entities, beneficial owners, directors, officers or authorized employees) that have been determined to be a PEP, or a family member or close known associate of a PEP;
- The Company has submitted a suspicious activity report ("SAR") for the client within the previous 24-months.

The details of the methodology and risk scoring can be found in Section 12 of the RBA Document.

8.7.2 CUSTOMER DUE DILIGENCE (CDD)

Arf's primary customer base constitutes of corporates. Corporate bodies are those which are registered with the local company registry in their country of incorporation.

As part of CDD, Arf always identifies the representative of the customer (legal entity). Identification of the representative is performed by real-time photo or video transmission which is ensured by Onfido.

In addition to identification of customer's representative, Arf collects main incorporation documents of the customer as well as the information necessary to understand the corporate's legal form, structure and ownership and seeks to identify and, where appropriate through the Company's risk-based approach, seeks to verify the information on the individuals who own or control the firm using accredited third party vendors such as Onfido and Salv. Arf collects the following information on the corporate:

- Extract from the Companies Register
- Certificate of Incorporation
    - Legal Company Name
    - Incorporation date (if available in this document)
- Articles/Memorandum of Association
- Company Information
    - Company registration number
    - Telephone Number
    - Registered address

- Trading address
- Mailing Address
- Principal Place of Business
- Date of Incorporation
- Country of Incorporation
- Tax ID
- PEP determination
- Operations in high risk/sanctioned countries
- Previous regulatory enforcement actions

- Ownership Information / Confirmation Statement or Equivalent.
  - For All Shareholders, UBOs, Directors and any Authorized Persons (any individuals who otherwise exercise control over the management of the company)
    - Full Name
    - Address
    - Date of Birth
    - E-Mail
    - Phone Number
    - Country of Tax Residence
    - Citizenship
  - For all UBOs (25%+ Shares or Voting Rights; in case of high-risk client – 10%+ Shares or Voting Rights) and Significant Shareholders (10%+ Shares)
    - % of Ownership

Full understanding of the ownership structure should be obtained, so that Arf can clearly assess any risks that would otherwise be obscured.

- Directors, Signatory and Persons of Significant Control
  - Proof of ID
    - Valid passport
    - National Identity Card
- UBO's - For Natural Persons
  - Proof of ID
    - Valid passport
    - National Identity Card

- Proof of Address
    - Personal Utility Bill (i.e. gas, electricity or water bill)
    - Current bank statements or credit /debit card statements (issued by a regulated financial sector firm in the UK, EU or an equivalent jurisdiction.)
    - Equivalent Document Issued by Central or Local Government Authority Department or Agency (i.e. council tax bill)
- Other Information Required
    - Nature of the Business (Including financial statements/accounts, expected payment frequencies etc.)
    - Customer Website
    - T&C's for Product
    - Customer Profile
    - Business Size
    - State of their financial balance
    - Flow of Funds

8.7.3 SANCTIONS, POLITICAL EXPOSURE, AND ADVERSE MEDIA COVERAGE

A sanction is a preventative measure often implemented by governments and international bodies to change behavior, prohibit illicit activity and curb undesirable actions by certain high-risk persons or groups. A sanctions list is a compilation of individual sanctions that can be applied to individuals, countries, groups or companies. Sanctions lists are often collated by governments or international bodies.

A politically exposed person (PEP) is an individual with a high-profile political role, or who has been entrusted with a prominent public function. PEP status does not predict criminal behavior, but the additional risk exposure it brings means that financial institutions must apply additional AML / CFT measures when establishing and during a business relationship. As a baseline, persons holding the following positions, or their family members or close associates, may be categorized as PEP:

- Government Officials: Current or former officials appointed to domestic government positions, or positions in a foreign government. This may include heads of state or individuals working in executive, legislative, administrative, military, or judicial branches, in elected and unelected roles, including but not limited to the Head of the State, the Head of the

Government, a minister, a vice-minister or a deputy minister, the State Secretary, the Chancellor of the Parliament or the Government or a ministry.

- Political Party Officials: Senior officials appointed to roles in major political parties at home or in foreign countries, including the head, deputy head, or member of a managing body of a political party.
- Senior Executives: Individuals serving in senior executive roles, such as directors or board members, in government-owned commercial enterprises or international organizations – that is corporations, businesses, or other entities formed by or for the benefit of any such individuals.
- Members of the Parliament;
- Courts: a member on the Supreme Courts, the Constitutional Courts or any other supreme judicial authorities whose decisions are not subject to appeal;
- Municipality: the mayor of a municipality, the head of a municipal administration;
- Audit Authority: a member of the management body of the supreme national audit and control body or the chairman, deputy chairman, or member of the board of a central bank;
- Armed Forces: an ambassador, a chargé d'affaires ad interim, Commander of the Lithuanian Armed Forces, Commanders of the Armed Forces and Units, Chief of Defence Unit or a high-ranking officer of the foreign armed forces;
- State or Municipal Entities: a member of a managing or supervisory body of a state-owned entity, public limited liability company, private limited liability company where the state owns shares or proportion of shares entitling to more than ½ of all votes at a general meeting of shareholders of said entities or companies; and / or a member of a managing or supervisory body of a municipal entity, public limited liability company, private limited liability company where the municipality owns shares or proportion of shares entitling to more than ½ of all votes at a general meeting of shareholders of said entities or companies and which are considered as large companies;
- International Organizations: the head or deputy head or member of a managing or supervisory body of an international intergovernmental organisation;
- Family Members: An immediate family member of a government or political official, or senior executive – meaning spouses, a person with whom partnership has been registered, parents, siblings, children, and spouses' of parents and siblings.

- **Close Associate:** A natural person who, together with a person who performs or has performed prominent public functions, is the participant of the same legal entity or the organisation without the status of legal entity or maintains other business relations; and / or a natural person who is the only Ultimate Beneficial Owner of a legal entity or an organisation without the status of legal entity that is established or operating de facto with a view to receive economic gain or other personal benefits for a person who performs or performed prominent public functions.

As part of its customer onboarding process, and on an ongoing basis, ARF will monitor all relevant sanctions and politically exposed persons -PEP- lists, applicable based on the profile of the customer, and at a minimum the sanctions lists maintained by the sanctioning bodies of the European Union, HM Treasury, US Office of Foreign Assets Control (OFAC) and the UN Security Council.

In addition to the checking such lists, ARF will strive, to the best extent possible, to determine whether the customer and/or its beneficial owner(s) are politically exposed, manually and by automated internal tools and real-time integration with expert third party services (that are in compliance with FATF requirements), through adverse media screening.

8.7.4 TRANSACTION MONITORING

Arf continuously monitors, through automated as well as manual systems, all account activity taking into consideration the risk profile of the customer and the type, complexity, purpose, volume and pattern of their transactions.

Arf strives to establish and develop an automated transaction monitoring system, comprising of internal systems integrated with expert third party services, that provides the ability to:

- monitor transactions and identify anomalies that might indicate suspicious activity,
- gather relevant due diligence information on both new and existing customers,
- conduct advanced evaluation and analysis of suspicious/unusual transactions,
- view individual transactions within the broader context of the customer's total activity,
- establish new and update existing risk-parameter settings and scenarios without requiring programming skills,
- establish workflow features that include automated alerts, simultaneous collaboration among designated units, escalation and reporting mechanisms,

- produce comprehensive reports for different consumers, including management and relevant regulators.

The monitoring aims to set proper flags, at a minimum, to the following type of transactions:

- transactions by customers with a high-risk profile,
- transactions to or from customers in high-risk geographies,
- transactions above determined thresholds,
- transactions ordered from previously unknown devices or new geolocations,
- transactions following a repeating pattern albeit below determined thresholds,
- complex and unusual transactions,
- transactions inconsistent with the customer's profile, business, or source of funds,
- and transactions that are flagged by the customized scenarios developed by Arf.

with relevant alerts and reports being distributed to designated units in the system with a proper audit trail.

The Compliance Unit will review any activity that the monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will file a Suspicious Activity Report (SAR) with appropriate authorities as described in Section 8 of this document.

8.7.5 ENHANCED DUE DILIGENCE (EDD)

If the Company determines that a client is high risk, based on the criteria contained in Section 12.1 of the RBA Document, the Company must take enhanced measures and request the following additional documentation:

For corporate clients:

- Management approval to enter into or maintain the business relationship
- Adverse media search for the client. (Subsequent adverse media searches are conducted for the client as part of the Company's ongoing monitoring efforts.)
- Identifying UBOs
- CDD Documentation (Passport copy, Proof of Address and other relevant documents) for Significant Shareholders with 10% ownership and above

- Detailed Business Plan including detailed product descriptions, pricing, geographies of operation etc.
- Documentation demonstrating purpose of select transactions
- Source of Wealth
- Detailed Flow of Funds
- Source of Funds (Where are the funds coming from (how will the account be funded – payment type, name of payer and bank/PSP name, Country of origin of payment, value of payment, what are the source of these funds (salary, gift etc.) - factor this into transaction monitoring rules in Salv)

For clients that are Financial Institutions (in addition to the above):

- AML Policy
- Complaints Policy
- IT Security Policy
- Governance Policy
- Organisation Structure Chart
- Compliance Monitoring and Implementation Plan
- Independent AML Audit

In addition to the documentation above the company sets Lower Value / Volume Limits in Transaction Monitoring. These limits are decided by the Chief Compliance Officer per client basis.

8.7.6 PERIODIC REVIEWS

Arf refreshes and reviews the due diligence information it holds on its clients on a risk sensitive basis. This takes place based on the outcome of the client's current risk assessment on the following scale:

- Low Risk Client - Every 3 years from date of original due diligence
- Medium Risk Client - Annually
- High Risk Client - Annually

Arf reviews the data obtained during the initial CDD for onboarding and ensure that the details that it holds are still up to date and accurate. Arf also refreshes the client risk assessment based on the

above-mentioned periods to ensure that the scoring assigned to each client is still up to date and accurate.

8.7.7 EVENT BASED REVIEWS

Outside the periodic review process there are a range of trigger events that require compliance to conduct a review of the client's CDD. Below are a series of examples that require a further review by compliance:

- The customer wants to utilise new functionality or open an account with a different product offered.
- Law Enforcement Requests
- The Company recently discovered that a UBO/Shareholder/Director/Authorized Person is a PEP.
- The client details/profile change:
  - Address details - may change risk profile and require EDD
  - Legal name - require screening and ongoing monitoring
  - Anticipated activity - need to understand why
  - Alerts are triggered (positive screening hits) may alter risk profile and require EDD
  - New product - understand the nature and purpose of the account

9 SUSPICIOUS ACTIVITY REPORTS (SAR)

9.1 PROCESS

All client transactions are subject to ongoing monitoring and review by the Chief Compliance Officer or delegates. Any director or employee who has any suspicion of money laundering by a person with whom Arf has any business dealings will immediately report the matter to the CCO. The reporting process and relevant triggers are defined in detail in Arf's **"Process Map KYC-AML Team"** document.

The CCO or delegate is obliged to raise an Internal SAR as soon as practicable if they consider that there is knowledge, suspicion, or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering, or that terrorist property exists. Having made such a report, the director or employee concerned will have met his or her legal obligations under the regulations. In addition to submitting an Internal SAR, the CCO is also obliged to immediately report the same information to UAB "PAYRNET" and provide any further assistance or information related to such

case provided that SAR is related to the client who is onboarded by Arf under its status of UAB "PAYRNET"'s distributor.

An employee may first discuss their suspicions with their line manager who may then accept responsibility for making a report to the MLRO. Any line manager who is approached by an employee to discuss a suspicious transaction or one known to involve money laundering must ensure that:

- the line manager himself or herself makes a report to the MLRO; or
- the employee who made the approach makes a report to the MLRO; or
- the line manager records his or her reasons for not making a report to the MLRO.

Arf ensures that all employees who handle payment or investment transactions of any kind (including back office staff) are given training in recognition and handling of suspicious Transactions and are aware of their individual responsibilities under the rules.

9.2 INFORMATION ON THE SAR

- Background/explanation of Arf's business (Specify product offerings and what products/services Arf provided/offered to the specific client).
- Completed details of the main subject/company and any associate companies as appropriate.
- Transaction details, if appropriate.
- Reason for suspicion:
    - Who is involved?
    - What are they doing?
    - At what stage is the activity?
- Source and beneficiary information for the activity and /or transaction.
- Company registration numbers (if known).
- Names of directors and positions held in the company/companies.
- Whether the company has subsidiaries, or holdings in other companies?
- Whether the company is itself a subsidiary and who its parent company is?
- What are the goods or activities being financed?
- Where are the goods currently located?
- Include as much unique data as is known:
    - Passport numbers
    - Driver's license numbers

- National Insurance numbers
- Car registration numbers
- Account numbers
- IBANs

Arf keeps an internal SAR log for record keeping and such files has limited access for only relevant individuals within the firm for information security purposes.

9.3 TIPPING OFF

It is a criminal offence for anyone in the regulated sector, following a disclosure to a nominated officer or to the appropriate agency, to do or say anything that might either 'tip off' another person that a disclosure has been made or prejudice an investigation.

Arf, as part of its staff training, makes certain all staff are aware of the requirement to submit suspicious activity reports where they have grounds for that suspicion and that they must not do or say anything to anyone about that report and its contents. When an account is the subject of a suspicious activity report, the CCO will mark it as 'high risk'. Care must be taken when speaking to a client whose account is so marked. Advice must be sought from the CCO as soon as possible.

9.4 ACCOUNT CLOSURE PROCEDURES (SAR FILED)

The decision as to whether or not Arf will keep an account open after a SAR has been filed will be made by the CCO on a case-by-case basis. The CCO will document the decision on whether to close or keep an account open. The following is the process to determine whether or not to keep an account open or to close:

- The CCO, after evaluating the customer's profile and transactional history in the account (as well as UAB "PAYRNET"'s opinion, if any was provided), will recommend closing the account, if in the opinion of the CCO:
    - The customer poses a risk to Arf or its partners as it has been identified as a person or entity directly linked to the crime
    - The conduct of the customer has led to the filing of more than two SARs
    - There is a risk for the type of customer activity, or any other pertinent situation
    - If the relationship could expose Arf or its partners to reputational, financial, legal, or operational risk, legal action, fines, or civil or criminal penalties
    - If UAB "PAYRNET" requested closing the account of the client.

Once it has been determined that an account needs to be closed, the following procedure will apply:

- Inform the customer that Arf can no longer provide services to them through a letter/email of dis-engagement. Reasons provided should not be construed as tipping off and must be generic such as internal changes of direction
- Lock the account
- If there are balances in the account, the customer must respond, in writing, requesting the balance be sent back to them. If the case involves or is suspected to be involved in money laundering or terrorist financing, then the balance may be frozen for such period as is reasonable whilst also liaising with any regulatory or law enforcement authority on next steps
- The customer will be required to provide KYC and/or KYB details for their account

Finally, inform the customer that the services of Arf must not be used by them, their company or companies affiliated with them.

10 COMPLAINTS

In order for Arf to investigate and deal with complaints in an efficient and effective manner, the complainant must provide their name, address and a telephone number on which Arf can contact them on. If the complainant is contacting Arf in writing, they should provide a clear description of their concerns or complaint and express their expectation of how they would like Arf to resolve it.

Arf shall acknowledge receipt of complaints in writing within three business days and endeavour to provide a resolution within 15 business days. However, from time to time, it may be necessary to carry out further investigations. If this occurs, Arf will inform the customer if their complaint is classified as warranting exceptional circumstances and indicate the reasons for the associated delay. Arf may require the maximum 35 days from the date of receipt of the complaint before responding to the complainant. However, Arf will keep the complainant updated on the progress of their complaint throughout.

11 RECORD KEEPING

Arf will document each step of the verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process and keep records containing a description of any document relied on to verify a customer's identity, noting the type of document, any identification number contained

in the document, the place of issuance, and if any, the date of issuance and expiration date. The record keeping is conducted including but not limited to the following items:

- Customer information
- Transactions
- Internal and external suspicion reports
- CCO annual (and other) reports
- Information not acted upon
- Training and compliance monitoring
- Information about the effectiveness of training

With respect to non-documentary verification, Arf will retain documents that describe the methods and the results of any measures taken to verify the identity of a customer.

Arf will also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained and will retain records of all identification information.

The CCO will conduct a periodic review to ensure that Arf is maintaining the records that are described in the policy.

All end-to-end client relationship records within the scope of AML/CTF Program will be maintained for a period of at a minimum 5 years, and all internal compliance records will be maintained for a period of 8 years, unless there is a longer period arising from any legislation or standards Arf adheres to, including requirements raised by UAB "PAYRNET" since the usual data storage term applied for UAB "PAYRNET" is 8 years (5 years is only applicable to correspondence with the client and letters and documents by which findings of the investigation of complicated or unusually large transactions and unusual structures of transactions are documented). Arf will also store the following logs which may be at anytime requested by UAB "PAYRNET":

(i) Log of monetary operations exceeding EUR 15,000 (both executed in cash and not in cash). It covers both one-off as well as related operations or transactions;

(ii) Log of clients with whom transactions or the business relationship have been terminated due to circumstances related to infringements of the procedure for the prevention of ML / TF, including cases when business relationship was terminated because clients or their representative(s) tried to conceal information about themselves or beneficial owners, did not provide all required information, etc.

Logs shall be stored for 8 years.

Please review Arf's **"Privacy Policy"** document for further details about data retention, transfers and security.

12 INDEPENDENT AUDIT

The AML/CTF Program will be audited, at least annually and whenever deemed necessary, by either a fully independent internal audit unit or by an independent third party competent in AML and CTF auditing.

The conducted audit will cover, at a minimum:

- A full review of the AML/CTF Program, including policies and procedures,
- A full review of the customer identification component,
- Testing and evaluation of the transaction monitoring component,
- Review of past escalations and SARs filed with authorities, if any,
- Evaluation of the training component,
- Review of past audit reports to assess the efficacy of recommended implemented changes.

While determining the scope of the audit, any inconveniences and risky customers, services and transactions determined by the AML/CTF Program will be included in the audit scope. Furthermore, the scope should include transactions of sufficient quantity and quality to represent the entire transactions performed by Arf.

The results of the conducted audit, including any determined imperfections, errors and misconduct revealed, the opinions and proposals for preventing recurrence of any such imperfections, errors and misconduct, will be reported directly to the Board of Directors.

13 TRAINING

All new Arf employees receive mandatory training on Arf's policies and procedures that constitute a part of the AML/CTF Program. All applicable employees are also required to complete further training annually. Participation in additional targeted trainings is required for all employees with day-to-day responsibilities relevant to AML/CTF Program.

The above-mentioned trainings cover, at a minimum:

- concepts of money laundering and financing of terrorism, and all related concepts, including methodologies used for such purposes with case studies,
- national and international regulations concerning anti-money laundering and financing of terrorism and crime, and
- how to identify flags and signs of money laundering that arise during the course of the employees' duties,
- what to do once the risk is identified (including how, when and through which organizational channels to escalate unusual customer activity or other red flags),
- what employees' roles are in Arf's compliance efforts and how to perform them,
- Arf's record retention policy, and
- the disciplinary consequences (including civil and criminal penalties) for non-compliance.

Arf's operations are regularly reviewed to check whether certain employees require specialized additional training. Written procedures are updated to reflect any such changes.

Arf also sets a periodic training, refreshing regime with the following structure:

- Arf provides training to staff upon return from an extended period of absence.
- Refresher training is provided to staff at least annually.
- Arf periodically reviews and updates the training materials.

Specific trainings may be also performed on an annual basis by UAB "PAYRNET" seeking to introduce Arf employees to UAB "PAYRNET" ML / TF prevention framework, new ML / TF prevention requirements introduced within UAB "PAYRNET"'s internal procedures, mandatory requirements to be applied by Arf as distributor of UAB "PAYRNET", etc.

APPENDIX A – REVISION HISTORY

Version	Date MM/DD/YYYY	Author	Reviewer	Description
2021/03-02	24/03/21	Rajpal S. Khangura (CCO)	Berhan Kongel	Addition of UAB "PAYRNET specific processes
2021/03-01	04/03/21	Rajpal S. Khangura (CCO)	Berhan Kongel	Addition of account closure and complaints
2021/01-01	28/01/21	Berhan Kongel	Kazım Rıfat Özyılmaz	First Version of Arf's New AML/CTF Policy

APPENDIX B – COUNTRY RISK RATINGS

Arf has based its country risk ratings on the methodology that is utilized by KnowYourCountry[1], an industry-recognized aggregator of geographic ML/TF risk information.

Arf also relies on the Countries' Risk Mapping of UAB "PAYRNET" which is mandatory to Arf and in case of any contradicting clauses between Countries' Risk Mapping of UAB "PAYRNET" and internal procedures of Arf, Countries' Risk Mapping of UAB "PAYRNET" shall prevail, except for cases when internal procedures of Arf assigns a higher risk to relevant country than is assigned under Countries' Risk Mapping of UAB "PAYRNET" – in such case higher risk assignment should be followed.

I. COUNTRIES' RISK MAPPING OF UAB "PAYRNET":

Sanction country	Country code	Prohibited country	Country code	High risk + EDD	Country code	High risk	Country code
Afghanistan	AF	Belarus	BY	Nigeria	NG	Algeria	DZ
Crimea	N/A	Central African Rep	CF	Puerto Rico	PR	Angola	AO
Cuba	Cu	Congo, the Democratic Republic	CD	Saudi Arabia	SA	Antigua and Barbuda	AG
Iran, Islamic Republic of	IR	Eritrea	ER	Sri Lanka	LK	Armenia	Am
North Korea	KP	Ethiopia	ET	Tunisia	TN	Azerbaijan	AZ
Syria	SY	Republic of Guinea	GN			Belize	BZ
Venezuela	VE	Iraq	IQ			Benin	BJ
		Lebanon	LB			Bolivia	BO
		Liberia	LR			Bosnia-Herzegovina	BA
		Libya	LY			Brazil	BR
		Mali	ML			British Virgin Islands	VG
		Myanmar	MM			Burundi	BI
		Pakistan	PK			Cape Verde	CV
		Russian Federation	RU			China	CV
		Somalia	SO			Colombia	CO
		South Sudan	SS			Comoros	KM

[1] https://www.knowyourcountry.com/country-ratings-table

		Sudan	SD			Curacao	CW
		Ukraine	UA			Dominica	DM
		Yemen	YE			Dominican Republic	DO
		Zimbabwe	ZW			Ecuador	EC
		Bahamas	BS			Egypt	EG
		Botswana	BW			El Salvador	SV
		Ghana	GH			Gaza Strip	PS
		Panama	PA			Guatemala	GT
		Barbados	BB			Guinea Bissau	GW
		Cambodia	KH			Haiti	HT
		Iceland	IS			Honduras	HN
		Jamaica	JM			India	IN
		Mongolia	MN			Kazakhstan	KZ
		Nicaragua	NI			Kenya	KE
		Uganda	UG			Kosovo	XK
		Albania	AL			Kyrgyzstan	KG
		Mauritius	MU			Lao People's Democratic Republic	LA
		Guam	GU			Mexico	MX
		American Samoa	AS			Moldova	MD
		Samoa	WS			Montenegro	ME
		Trinidad & Tobago	TT			Morocco	MA
		United States Virgin Islands	VI			Mozambique	MZ
		Cayman Islands	KY			Paraguay	PY
		Palau	PW			Philippines	PH
		Vanuatu	VU			Serbia	RS
		Seychelles	SC			Sierra Leone	SL
		Fiji	FJ			St Kitts & Nevis	KN
		Oman	OM			St Lucia	LC
						St Maarten	SX
						St Vincent & Gren	VC
						Tajikistan	TJ
						Tanzania	TZ
						Thailand	TH
						Turkey	TR
						Turkmenistan	TM
						Uzbekistan	UZ
						Vietnam	VN

						West Bank (Palestinian Territory)	PS
						Western Sahara	EH

Risk level	Trading address	Registration address	Residency Address	Owner / Director residency	Send / Receive Money	EDD on All Payments
High + EDD	Yes	Yes	Yes	Yes	Yes	Yes
Prohibited	No	No	No	Yes	No	No
Sanctioned	No	No	No	No	No	No

II. INDIVIDUAL ARF COUNTRIES" RISK MAPPING:

KnowYourCountry assigns a risk score to each country based on a consideration of the following:

- Countries that have been designated as uncooperative or deficient by the Financial Action Task Force ("FATF");
- The degree to which a country is in compliance with the FATF's recommendations;
- Countries' inclusion on lists of jurisdictions of primary concerns for money laundering or support of terrorism that are prepared by the US State Department;
- Whether the country is the subject of international sanctions;
- The corruption assessments prepared by Transparency International and the World Bank;
- The assessment of the effectiveness of a country's governance structure as determined by the World Bank;
- Countries that have been included on a list of major drug transit or major illicit drug producing countries, prepared by the US President;

- The degree to which countries comply with the standards set by the Trafficking Victims Protection Act; and
- Countries that have been identified as an Offshore Financial Centre.

Based on the above factors, KnowYourCountry assigns a score between 0 and 100 to each country, which translates to the following risk ratings:

Score	Risk Rating
<50.00	High
50.00 – 59.99	Medium-High
60.00 – 69.99	Medium
70.00 – 79.99	Medium-Low
80.00 – 100	Low

Arf prohibits transactions involving countries that are the target of EU sanctions or evaluated as such by Arf's banking partners, regardless of the risk score that is assessed by KnowYourCountry. For more information about KnowYourCountry's country risk rating methodology, refer to https://www.knowyourcountry.com

The following ratings are current as of January 2021.

Country	Score	Arf Score	Index
Sweden	87.56	Low-Risk	1
Norway	87.49	Low-Risk	1
Svalbard and Mayen	87.49	Low-Risk	1
Åland Islands	86.64	Low-Risk	1
Finland	86.64	Low-Risk	1
New Zealand	85.87	Low-Risk	1
Tokelau	85.87	Low-Risk	1

Denmark	85.63	Low-Risk	1
Faroe islands	85.63	Low-Risk	1
Greenland	85.63	Low-Risk	1
Estonia	84.57	Low-Risk	1
Slovenia	83.79	Low-Risk	1
Lithuania	83.56	Low-Risk	1
Bermuda	83.4	Low-Risk	1
Andorra	82.39	Low-Risk	1
San Marino	81.9	Low-Risk	1
Malta	81.47	Low-Risk	1
Austria	79.97	Medium-Low Risk	2
Croatia	79.93	Medium-Low Risk	2
Namibia	78.36	Medium-Low Risk	2
Vatican City State (Holy See)	77.99	Medium-Low Risk	2
South Korea	77.94	Medium-Low Risk	2
Germany	77.82	Medium-Low Risk	2
France	77.69	Medium-Low Risk	2
French Guiana	77.69	Medium-Low Risk	2
French Polynesia	77.69	Medium-Low Risk	2
Guadeloupe	77.69	Medium-Low Risk	2
Martinique	77.69	Medium-Low Risk	2
Mayotte	77.69	Medium-Low Risk	2
New Caledonia	77.69	Medium-Low Risk	2
Réunion	77.69	Medium-Low Risk	2
Saint Berthélemy	77.69	Medium-Low Risk	2
Saint Martin (French part)	77.69	Medium-Low Risk	2
Saint Pierre and Miquelon	77.69	Medium-Low Risk	2
Wallis and Futuna	77.69	Medium-Low Risk	2
Burkina Faso	77.58	Medium-Low Risk	2
Montserrat	77.55	Medium-Low Risk	2
Bhutan	77.42	Medium-Low Risk	2
Rwanda	77.09	Medium-Low Risk	2
Macedonia	77.09	Medium-Low Risk	2
Australia	76.88	Medium-Low Risk	2
Christmas Island	76.88	Medium-Low Risk	2

Cocos (Keeling) Islands	76.88	Medium-Low Risk	2
Norfolk Island	76.88	Medium-Low Risk	2
Malawi	76.87	Medium-Low Risk	2
Singapore	76.83	Medium-Low Risk	2
Brunei Darussalam	76.81	Medium-Low Risk	2
Solomon Islands	76.76	Medium-Low Risk	2
Switzerland	76.63	Medium-Low Risk	2
Zambia	76.5	Medium-Low Risk	2
Guernsey	76.44	Medium-Low Risk	2
Czech Republic	76.32	Medium-Low Risk	2
Anguilla	76.16	Medium-Low Risk	2
Latvia	76.11	Medium-Low Risk	2
Chile	76.09	Medium-Low Risk	2
Belgium	76.01	Medium-Low Risk	2
Greece	75.61	Medium-Low Risk	2
Tonga	75.56	Medium-Low Risk	2
Niue	75.52	Medium-Low Risk	2
Liechtenstein	75.42	Medium-Low Risk	2
Ireland	75.42	Medium-Low Risk	2
Qatar	75.36	Medium-Low Risk	2
Jersey	75.34	Medium-Low Risk	2
Spain	75.33	Medium-Low Risk	2
Canada	75.16	Medium-Low Risk	2
Mauritania	75.13	Medium-Low Risk	2
Luxembourg	74.82	Medium-Low Risk	2
Taiwan	74.72	Medium-Low Risk	2
Isle Of Man	74.65	Medium-Low Risk	2
North Mariana Islands	74.64	Medium-Low Risk	2
United States	74.64	Medium-Low Risk	2
Poland	74.46	Medium-Low Risk	2
British Indian Ocean Territory	74.38	Medium-Low Risk	2
Falkland Islands (Malvinas)	74.38	Medium-Low Risk	2
Pitcairn	74.38	Medium-Low Risk	2
Saint Helena, Ascension and Trista	74.38	Medium-Low Risk	2
United Kingdom	74.38	Medium-Low Risk	2

Portugal	74.17	Medium-Low Risk	2
Slovakia	74.15	Medium-Low Risk	2
Uruguay	74.13	Medium-Low Risk	2
Hungary	74.08	Medium-Low Risk	2
Lesotho	74.01	Medium-Low Risk	2
Bulgaria	73.65	Medium-Low Risk	2
South Africa	73.31	Medium-Low Risk	2
Niger	73.26	Medium-Low Risk	2
Marshall Islands	73.24	Medium-Low Risk	2
Micronesia	73.12	Medium-Low Risk	2
Madagascar	73.04	Medium-Low Risk	2
Togo	72.87	Medium-Low Risk	2
Nepal	72.66	Medium-Low Risk	2
Cook Islands	72.6	Medium-Low Risk	2
Kuwait	72.57	Medium-Low Risk	2
Italy	72.41	Medium-Low Risk	2
Gabon	72.32	Medium-Low Risk	2
Gibraltar	72.02	Medium-Low Risk	2
Bonaire, Sint Eustatius and Saba	71.93	Medium-Low Risk	2
Netherlands	71.93	Medium-Low Risk	2
Nauru	71.93	Medium-Low Risk	2
Romania	71.77	Medium-Low Risk	2
Georgia	71.69	Medium-Low Risk	2
Papua New Guinea	71.38	Medium-Low Risk	2
Cameroon	71.32	Medium-Low Risk	2
Monaco	71.31	Medium-Low Risk	2
Congo (Brazzaville)	70.6	Medium-Low Risk	2
Maldives	70.59	Medium-Low Risk	2
Bahrain	70.54	Medium-Low Risk	2
Gambia	70.51	Medium-Low Risk	2
Turks & Caicos	70.41	Medium-Low Risk	2
Chad	70.27	Medium-Low Risk	2
Bangladesh	70.13	Medium-Low Risk	2
Equatorial Guinea	70.01	Medium-Low Risk	2
Costa Rica	69.95	Medium Risk	3

Grenada	69.84	Medium Risk	3
Swaziland (Eswatini)	69.78	Medium Risk	3
Hong Kong	69.78	Medium Risk	3
Macau	69.5	Medium Risk	3
Tuvalu	69.46	Medium Risk	3
Cyprus	69.29	Medium Risk	3
Argentina	69.2	Medium Risk	3
Timor-Leste	69.13	Medium Risk	3
Jordan	68.94	Medium Risk	3
Guyana	68.88	Medium Risk	3
Israel	68.73	Medium Risk	3
Indonesia	68.49	Medium Risk	3
Aruba	68.39	Medium Risk	3
United Arab Emirates	68.35	Medium Risk	3
Kiribati	67.93	Medium Risk	3
Cote D'Ivoire	67.46	Medium Risk	3
Suriname	67.39	Medium Risk	3
Malaysia	67.03	Medium Risk	3
Djibouti	66.84	Medium Risk	3
Peru	66.75	Medium Risk	3
Japan	66.73	Medium Risk	3
Sao Tome & Prin.	66.38	Medium Risk	3
Senegal	66.24	Medium Risk	3
Dominica	63.03	Medium Risk	3
Guinea	61.62	Medium Risk	3
British Virgin Islands	67.05	High Risk	4
Kazakhstan	66.93	High Risk	4
Sierra Leone	66.85	High Risk	4
Angola	66.74	High Risk	4
St Kitts & Nevis	66.66	High Risk	4
Antigua and Barbuda	66.57	High Risk	4
Cape Verde	65.93	High Risk	4
India	65.87	High Risk	4
Kyrgyzstan	65.64	High Risk	4
St Vincent & Gren	65.23	High Risk	4

Curacao	64.80	High Risk	4
Algeria	64.79	High Risk	4
Serbia	64.75	High Risk	4
El Salvador	64.74	High Risk	4
Dominican Republic	64.70	High Risk	4
Thailand	64.66	High Risk	4
Tajikistan	64.64	High Risk	4
Montenegro	64.43	High Risk	4
Uzbekistan	64.20	High Risk	4
Honduras	64.15	High Risk	4
Benin	64.09	High Risk	4
Moldova	64.09	High Risk	4
Mexico	63.97	High Risk	4
Belize	63.89	High Risk	4
St Lucia	63.43	High Risk	4
Colombia	63.31	High Risk	4
Vietnam	63.26	High Risk	4
Tanzania	62.63	High Risk	4
Turkmenistan	62.49	High Risk	4
Paraguay	62.25	High Risk	4
Armenia	62.24	High Risk	4
Kosovo	62.07	High Risk	4
Kenya	61.83	High Risk	4
Mozambique	61.02	High Risk	4
Guatemala	60.29	High Risk	4
Morocco	60.25	High Risk	4
Western Sahara	60.25	High Risk	4
Bolivia	59.83	High Risk	4
Philippines	59.68	High Risk	4
Comoros	59.52	High Risk	4
Lao People's Democratic Republic	58.94	High Risk	4
China	58.72	High Risk	4
Ecuador	58.49	High Risk	4
Azerbaijan	56.89	High Risk	4
Egypt	56.52	High Risk	4

West Bank (Palestinian Territory, O	56.44	High Risk	4
Brazil	56.30	High Risk	4
Gaza Strip	55.54	High Risk	4
Turkey	55.16	High Risk	4
St Maarten	54.46	High Risk	4
Burundi	54.04	High Risk	4
Bosnia-Herzegovina	52.06	High Risk	4
Guinea Bissau	48.59	High Risk	4
Haiti	48.00	High Risk	4
Sri Lanka	71.49	High Risk + EDD	5
Puerto Rico	68.94	High Risk + EDD	5
Saudi Arabia	68.70	High Risk + EDD	5
Tunisia	59.20	High Risk + EDD	5
Nigeria	55.28	High Risk + EDD	5
Iceland	85.10	Prohibited	6
Oman	80.41	Prohibited	6
Fiji	76.40	Prohibited	6
Mongolia	75.27	Prohibited	6
American Samoa	72.99	Prohibited	6
Ethiopia	71.56	Prohibited	6
United States Virgin Islands	70.99	Prohibited	6
Cayman Islands	68.05	Prohibited	6
Guam	67.90	Prohibited	6
Palau	66.90	Prohibited	6
Bahamas	66.28	Prohibited	6
Seychelles	65.28	Prohibited	6
Vanuatu	64.60	Prohibited	6
Trinidad & Tobago	64.52	Prohibited	6
Eritrea	64.19	Prohibited	6
Belarus	62.90	Prohibited	6
Samoa	60.83	Prohibited	6
Mali	59.22	Prohibited	6
Uganda	58.83	Prohibited	6
Ukraine	57.12	Prohibited	6
Liberia	56.94	Prohibited	6

Central African Rep	56.57	Prohibited	6
Russian Federation	56.20	Prohibited	6
Sudan	54.83	Prohibited	6
Albania	53.68	Prohibited	6
Cambodia	53.15	Prohibited	6
Jamaica	52.49	Prohibited	6
Ghana	50.70	Prohibited	6
Congo, the Democratic Republic	49.45	Prohibited	6
Barbados	48.01	Prohibited	6
Lebanon	46.08	Prohibited	6
Zimbabwe	44.81	Prohibited	6
Libya	44.60	Prohibited	6
South Sudan	44.50	Prohibited	6
Panama	43.84	Prohibited	6
Iraq	43.71	Prohibited	6
Pakistan	42.54	Prohibited	6
Somalia	38.00	Prohibited	6
Nicaragua	36.73	Prohibited	6
Myanmar	36.04	Prohibited	6
Yemen	32.89	Prohibited	6
Mauritius	32.89	Prohibited	6
Botswana	32.89	Prohibited	6
Cuba	54.04	Sanctioned	7
Venezuela	45.76	Sanctioned	7
Syria	34.89	Sanctioned	7
Afghanistan	32.10	Sanctioned	7
North Korea	20.93	Sanctioned	7
Iran, Islamic Republic of	17.83	Sanctioned	7

APPENDIX C – PROHIBITED & HIGH-RISK ENTITIES

Arf considers the following industries to be prohibited and does not conduct business with individuals or entities in these industries:

- Unregulated financial services (where licensing required)
- Pyramid or Ponzi scheme or multi-level marketing programs
- Hawala
- Un-licensed FX broker
- Binary options
- Debt restructuring, credit repair, debt settlement, providing credit, debt collections, (unless received a written pre-approval from Arf)
- Gambling [1]
- Get rich quick scheme [2]
- Activities aimed at circumventing security controls (software, hardware)
- Unregulated pharmaceuticals / food supplements (e.g.“nutraceuticals”) [3]
- Piracy or illegal streaming
- Counterfeit goods and violation of intellectual property, items that violates someone's privacy
- Arms / dual use goods/ human organs
- Unlicensed charities
- Shell companies
- Companies formed of Bearer Shares
- Remittances funded in cash; Cash and Check Handling: Check Cashing, Deposit Taking, Cash Transfer.
- Offshore bank transactions/ Shell banks [4]
- Adult services connected to human trafficking; intermediation of prostitution; production, visual broadcasting of pornography or striptease clubs (the approach does not include literature, toys, DVD's, educational or scientific material or dating sites)
- Fourth party payment & multi-layered MSB arrangements
- Transactions for goods subject to export prohibition/restrictions
- Transactions with living animals (exceptions possible like for payments for horse riding, or dog classes)
- Political / religious organisations engaged in hate speech [5]
- Sanctioned entities

The Company considers the following industries or business models to be high risk and assigns risk points to those individuals and entities:

- Accounting Firms
- Holding Companies
- Cross border transportation companies
- Importer/Exporter
- Cash intensive businesses (e.g. nail salon, convenience store, restaurant)
- Art gallery/dealer
- Auto/Boat/Motorcycle/RV Dealer
- Pawn shops
- Not for profit organizations
- Chemical manufacturer or processors
- Real estate developers or brokers
- Dealer in precious metals or stones
- Parking lot owners/parking lot management companies

- [1] Gambling and any similar activity with an entry fee and/or monetary prize, including, but not limited to casino games, sports betting, horse or greyhound racing, fantasy sports, lottery tickets, other ventures that facilitate gambling
- [2] Short term investment for very high return
- [3] Drugs, narcotics, steroids, other products with danger to health. Homemade alcoholic beverages, cigarettes and tobacco
- [4] Offshore refers to the EU commission tax evasion blacklist and grey list https://ec.europa.eu/taxation_customs/tax-common-eu-list_en.
- Any exceptions need to be approved by the CCO/MLRO
- [5] Selling, hosting, distributing, producing or promoting offensive materials, including materials that incites racial hatred or promotes discrimination based on gender, race, religion, national origin, physical ability, sexual orientation, or age