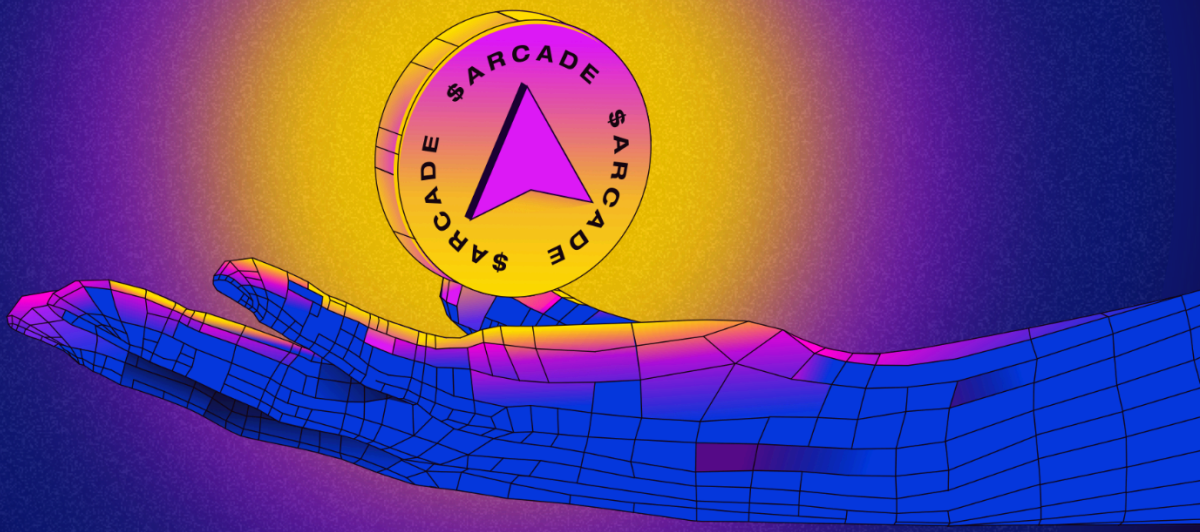
ARCADE

THE LEADING GAME-FI PLATFORM

KNOW YOUR CUSTOMERS ANTI-MONEY LAUNDERING

POLICY & PROCEDURES



ARCADE2EARN LTD
COMPLIANCE & SUPERVISORY PROCEDURES

SECTION 1. BOARD DIRECTIVE

All subsidiaries, sister companies, and/or affiliates of Arcade2Earn LTD (collectively referred to as "**Arcade**") shall establish an Anti-Money Laundering (or "**AML**") Program, also known as, Know Your Customers (or "**KYC**"), that at a minimum:

1. Develops internal policies, procedures, and reasonable control over documentation;
    a. In accordance with the Financial Crimes Enforcement Network (or "**FinCEN**")'s requirement that all nonbank financial institutions implement an Anti-Money Laundering program, effective compliance date of **August 13, 2012**.
2. Designates a compliance officer, who will be responsible for ensuring that:
    a. Arcade's AML Program is implemented effectively, including monitoring compliance by Arcade's agents, subsidiaries, sister companies, and affiliates within their obligations under the program;
    b. The AML Program is updated, as necessary; and
    c. Appropriate persons are educated and properly trained.
3. Offers ongoing employee training program;
    a. Arcade's Operations & Legal Department shall be responsible for collaborating to provide Arcade and its employees with ongoing training opportunities through third party training services, as necessary.

AND

4. Establishes an Independent Audit Function to test for compliance.

a. Arcade's Administrative and Technology Departments shall be responsible for collaborating to provide for independent testing to monitor and maintain an adequate AML Program, including but not limited to, testing to determine compliance of Arcade's agents, subsidiaries, sister companies, and affiliates with their obligations under the AML Program. The scope and frequency of the testing must be commensurate with the risks posed by the Arcade's products and services. Such testing may be conducted by a third party or by any officer or employee of Arcade, other than the person designated as the designated compliance officer. This could be a staff person, board member, and/or volunteer accounting or banking associate.

b. For additional background information see:

   i. http://nationalmortgageprofessional.com/news29200/anti-money-laundering-debuts-non-banks; and/or

   ii. The Federal Registry with the Final Rule: http://www.gpo.gov/fdsys/pkg/FR-2012-02-14/pdf/2012-3074.pdf

SECTION 2. AML POLICY STATEMENT

It is the policy of Arcade to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorists or criminal activity.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origin of criminally derived proceeds, so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages:

1. **Placement**: Cash generated from criminal activities is converted into monetary instruments, such as money orders or cryptocurrency, or deposited into accounts at financial institutions;

2. **Layering**: Funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin; and
3. **Integration**: Funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes. Because Arcade and its affiliated organizations may originate financial products, such as cryptocurrencies, NFTs, and other digital financial products, to be purchased on behalf of consumers, there is a very small but real risk of criminal activity through the purchase of assets in the form of cryptographic assets.

SECTION 3. AML COMPLIANCE OFFICER DESIGNATION & DUTIES

As required under the USA Patriot Act of 2001 (or the "**PATRIOT Act**"), Arcade designates **Jaleel Menifee, *Esq***., the Chief Operating Officer and General Counsel, as the Anti-Money Laundering Program Compliance Officer (or the "**AMLCO**"), with full responsibility for Arcade's AML Program. The AMLCO shall ensure:

1. Arcade's AML Program is implemented effectively, including monitoring compliance by Arcade's agents, subsidiaries, sister companies, and affiliates within their obligations under the program;
2. The AML Program is updated, as necessary; and,
3. The appropriate persons are educated and properly trained.

SECTION 4. SHARING AML INFORMATION WITH FEDERAL LAW ENFORCEMENT AGENCIES

We will respond to any FinCEN request about accounts or transactions by immediately searching our records to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity, or organization named in FinCEN's request. Upon receiving an information request, the AMLCO is to be responsible for responding to the request and similar requests in the future. Unless otherwise stated in FinCEN's request, we are required

to search current accounts and transactions, accounts maintained by a named suspect during the preceding twelve (12) months, and transactions conducted by or on behalf of or with a named subject during the preceding six (6) months. If we find a match, we will report it to FinCEN by completing FinCEN's subject information form in a timely manner. If we search our records and do not uncover a matching account or transaction, then we will not reply as allowed under Section 314(a) of the PATRIOT Act.

We will not disclose the fact that FinCEN has requested or obtained information from us, except to the extent necessary to comply with the information request. We will maintain procedures to protect the security and confidentiality of requests from FinCEN, as required by Section 501 of the Gramm-Leach-Bliley Act.

4.1 Sharing AML Information with Federal Law Enforcement Agencies:

Prior to approving any application that potentially may involve money laundering, we will check to ensure that an applicant does not appear on the Treasury's OFAC "Specifically Designated Nationals and Blocked Persons" (or the "**SDN**") List, and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC website.

1. For more information, see:

    a. www.treas.gov/offices/enforcement/ofac/sdn/index.html

In the event that we determine an applicant, or someone with or for whom the applicant is transacting, is on the SDN List or is from or engaging in transactions with a person or entity located in an embargoed country or region, we will reject the application, and if there is sufficient concern, we may also call the OFAC Hotline at 1800-540-6322.

SECTION 5. APPLICANT IDENTIFICATION AND VERIFICATION

We have established, documented, and maintained a written Applicant Identification Program. We will collect certain minimum applicant identification information from each applicant and provide notice to applicants that we will seek

identification information and compare applicant identification information with government-provided lists of suspected terrorists as mentioned above in Section 4.

5.1 Required Applicant Information:

Prior to approving an application, we will collect the following information for all applicants:

1. The name;
2. An address, (which will be a residential or business street address for an individual), an Army Post Office ("**APO**") or Fleet Post Office ("**FPO**") number;
3. An identification number, which will be a taxpayer identification number (for U.S. persons), or one or more of the following:
    a. A taxpayer identification number, passport number, and country of issuance;
    b. Alien identification card number or number and country of issuance of any other government-issued document evidencing nationality, or
    c. Residence and bearing a photograph or other similar safeguard (for non-U.S. persons).

We will not approve an application in the event that an applicant has applied for, but has not received a taxpayer identification number and cannot prove his/her identity to the satisfaction of the AMLCO.

1. Agents of Arcade may refer non-U.S. applicants without an Individual Tax Identification Number to:
    a. http://www.irs.gov/individuals/article/0,,id=222209,00.html; and
    b. the most current W7 form on the IRS website for instructions on how to apply for a Taxpayer Identification Number: http://www.irs.gov/pub/irs-pdf/fw7.pdf

5.2 Applicants Who Refuse To Provide Information:

If a potential or existing applicant either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, Arcade will reject the application. In either case, our AMLCO will be notified, so that we can determine whether we should report the situation to FinCEN (i.e., file a Form SAR).

1. For a copy of the Suspicious Activity Report (or "**SAR**") see:
    a. http://bsaefiling.fincen.treas.gov/main.html

5.3 Verification of Information:

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of all applicants by using risk-based procedures to verify and document the accuracy of the information we receive regarding our applicants. In verifying applicant identity, we will analyze any logical inconsistencies in the information we obtain.

We will verify applicant identity through documentary evidence, non-documentary evidence, or both. We will use documents to verify applicant identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever possible. We may also use such non-documentary means, after using documentary evidence, if we are still uncertain about whether we know the true identity of the applicant. In analyzing the verification information, we will consider whether there is a logical consistency among the identifying information provided, such as the applicant's name, street address, zip code, telephone number (if provided), date of birth, and social security number.

Appropriate documents for verifying the identity of applicants include, but are not limited to, the following:

1. For an individual, an unexpired government-issued identification evidencing nationality, residence, and bearing a photograph or similar safeguard, such as a driver's license or passport; and

2. We understand that we are not required to take steps to determine whether the document that the applicant has provided to us for identity verification has been validly issued and that we may rely on a government-issued identification as verification of an applicant's identity; however, if we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the applicant's true identity.

We may use any or all of following non-documentary methods of verifying identity:

1. Contacting an applicant;
2. Independently verifying the applicant's identity through the comparison of information provided by the applicant with information obtained from a consumer reporting agency, public database, employer or other source; and/or
3. Checking references with financial institutions.

We will use non-documentary methods of verification in the following situations:

1. When the applicant is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard;
2. When Arcade's review is unfamiliar with the documents the applicant presents for identification verification; and/or
3. When there are other circumstances that increase the risk that Arcade will be unable to verify the true identity of the applicant through documentary means.

5.5 Recordkeeping:

We will maintain records of all identification information and verification information obtained for five (5) years after the application is received.

5.6 Notice to Applicants:

This AML Policy is publicly accessible from the Arcade Platform at:

www.Arcade2earn.io.

By accessing the Arcade Platform, applicants acknowledge that this AML Policy shall be considered to have placed said applicant on notice that Arcade is requesting information from said applicant to verify their identity, as required by Federal law. This AML Policy gives notice to applicants regarding Arcade's AML/KYC policies. Additionally, from time to time, Arcade will provide plainly posed notices that inform applicants of Arcade's AML Policy, such as:

"**To help the government fight the funding of terrorism and money laundering activities, Federal law requires us to obtain, verify, and record information that identifies each person who applies to purchase a financial product from Arcade. We will ask for your name, address and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents**."

SECTION 6. FOREIGN CORRESPONDENT ACCOUNTS AND SHELL BANKS

It is our policy that Arcade will not provide any financial products, such as cryptocurrencies, NFTs, and other cryptographic financial products, when we have a reasonable cause to believe a foreign bank or foreign financial institution is involved in any way with transacting purchases that are suspected to violate, or have violated, the PATRIOTS Act.

SECTION 7. MONITORING TRANSACTIONS FOR SUSPICIOUS ACTIVITY

7.1 Detecting Red Flags:

Red flags that signal possible money laundering or terrorist financing include, but are not limited to:

1. The applicant exhibits unusual concern about Arcade's compliance with government reporting requirements and its AML policies; is reluctant or refuses to reveal any information concerning personal finances; or furnishes unusual or suspicious identification or documents;

2. The information provided by the applicant that identifies a legitimate source for funds is false, misleading, or substantially incorrect;
3. Upon request, the applicant refuses to identify or fails to indicate any legitimate source for his or her funds and other assets when making large purchases;
4. The applicant (or a person publicly associated with the applicant) has a questionable background, or is the subject of news reports indicating possible criminal, civil, or regulatory violations;
5. The applicant exhibits a lack of concern regarding investment costs;
6. The applicant has difficulty describing the nature of his or her business;
7. The applicant makes unexplained or sudden purchases involving cash or cash equivalents, or other monetary instruments that appear to be structured to avoid the $10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds (for example, purchasing financial products in $9,950 increments);
8. The applicant requests that a transaction be processed to avoid the Arcade's normal documentation requirements; and/or
9. The applicant has inflows of funds or other assets well beyond the known income or resources of the applicant.

7.2 Responding to Red Flags and Suspicious Activity:

When an Agent of Arcade detects any red flags, he or she will investigate further under the direction of the AMLCO. This may include gathering additional information internally or from third-party sources, contacting the government or filing a Form SAR. Arcade shall be obligated to report suspicious transactions that are conducted or attempted by, at or through financial products, such as cryptocurrencies, NFTs, and other digital financial products, or a finance company, and involve or aggregate at least $5,000 in funds or other assets. We recognize that transactions are reportable

under 31 U.S.C. 5318(g) regardless of whether they involve currency. In such incidents, a SAR report will be filed no later than thirty (30) days after initial detection.

Arcade is provided with the same "safe harbor" as provided for other financial institutions, recognizing they must feel free to report suspicious transactions, and to share information in the employment context about individuals involved in misconduct, without fear of liability.

7.2(b) Currency Transaction Reports (or "**CTR**") – $10,000 Threshold:

Arcade shall file a report with the Internal Revenue Service within fifteen (15) days of receiving currency of more than $10,000 in one transaction, or in two or more related transactions occurring in a twelve (12) month period. The term "currency" includes coins and paper money, cashier's checks, money orders, bank drafts, traveler's checks, and any form of digital currency. It does not include personal checks. Contrary to the SAR confidentiality requirements, anyone involved in the transaction must be notified with a written statement that a report is being filed.

1. The form IRS Form 8300 can be found here:
    a. http://www.irs.gov/pub/irs-pdf/f8300.pdf.

SECTION 8. AML RECORD KEEPING

8.1 SAR Maintenance and Confidentiality:

We will hold SAR and any supporting documentation confidential. We will not inform anyone outside of a law enforcement or regulatory agency about a SAR. We will segregate SAR filings and copies of supporting documentation from other Arcade books and records to avoid disclosing SAR filings.

8.2 Responsibility for AML Records and SAR Filing:

Our AMLCO and his or her designee will be responsible to ensure that AML records are maintained properly and that any SARs are filed as required.

8.3 Records Required:

As part of our AML program, Arcade shall create and maintain SAR and other relevant documentation on applicant identity and verification (see **Section IV** above); and fund transfers and transmittals as well as any records related to applicants listed on the OFAC list. We will maintain SAR and their accompanying documentation for at least five (5) years.

SECTION 9. TRAINING PROGRAMS

Arcade's Operations Department shall provide Arcade's agents, subsidiaries, sister companies, and affiliates with ongoing training opportunities through appropriate third party training services, as necessary.

Furthermore, we shall review our operations to see if certain officers or employees require specialized additional training. Our written procedures will be updated to reflect any such changes.

SECTION 10. PROGRAM TO TEST AML PROGRAM

Annual testing of our AML program will be performed either by a qualified independent third party or internally by a qualified officer of Arcade. The annual testing will include an audit of our compliance with our AML program.

The auditor will issue a report of the auditor's findings upon completion of their audit to the Board of Directors, addressing each of the resulting recommendations.

SECTION 11. MONITORING EMPLOYEE CONDUCT AND ACCOUNTS

We will subject employee money service transactions to the same AML procedures as applicant accounts, under the supervision of the AMLCO. The AMLCO's accounts will be reviewed by a qualified member of Arcade's Ethics Committee.

SECTION 12. CONFIDENTIAL REPORTING OF AML NON-COMPLIANCE

Employees will report any violations of the Arcade's AML Program to the AMLCO, unless the violations implicate the AMLCO, in which case the employee shall report to an appropriate member of senior management. Such reports will be confidential, and the employee shall **NOT** suffer retaliation for making them.

SECTION 13. ADDITIONAL AREAS OF RISK

Arcade, and its designated AMLCO, has reviewed all areas of its business to identify potential money laundering risks that may not be covered in the procedures described above and is continually working to improve its AML Program.

SECTION 14. BOARD OF DIRECTORS' APPROVAL

The Board of Directors have approved this AML Program as reasonably designed to achieve and monitor Arcade's ongoing compliance with the requirements of the FinCEN extension of the AML/KYC requirements for non-bank, financial institutions.