SANCTIONS POLICY

Acuity Coaching

Document Version Control

Name	Sanctions Policy		
Status	Final		
Associated Policies			
Version No.	SP/02/23		
Last Updated	12th February 2023	**Next Review Date**	11th February 2024

www.acuitycoaching.com
Registered address: 130 Helmshore Road, Holcombe Village, Bury, Lancs BL8 4PB, UK

Hold Ctrl + Click on the section title to be taken directly to that section in the document

CONTENTS

1.0 INTRODUCTION

1.1 Objective

Acuity Coaching Ltd (Acuity) has responsibilities in the legal, regulatory, moral and social senses. In ensuring its compliance with these responsibilities, Acuity is clear in the objectives of this Sanctions Policy; namely assisting in the prevention of practices which are or could reasonably be construed as supporting countries / territories / regimes in which state sponsored unethical / immoral practices exist.

1.2 Furthermore, this Policy sets out to:

1.2.1 Provide a minimum benchmark of standards around a framework of core requirements;

1.2.2 Provide a consistent and effective approach to the application of sanctions;

1.2.3 Ensure compliance with applicable sanctions prevailing in the jurisdictions in which the Group operates; and

1.2.4 Articulate Acuity's position on related prohibitions and restrictions involving certain countries and territories.

2.0 DEFINITION (SANCTIONS)

2.1 Normally used by the international community for one or more of the following reasons:

2.1.1 To encourage a change in behaviour of a target country or regime

2.1.2 To apply pressure on a target country to comply with set objectives

2.1.3 As an enforcement tool when international peace and security has been threatened and diplomatic efforts have failed

2.1.4 To prevent and suppress the financing of terrorists and terrorist acts.

2.2 Financial sanctions are normally one element of a package of measures used to achieve one or more of the above. Financial sanctions measures can vary from the comprehensive – prohibiting the transfer of funds to a sanctioned country and freezing the assets of a government, the corporate entities and residents of the target country – to targeted asset freezes on individuals/entities.

2.3 **Definition (Financial and Trade Sanctions (Sanctions))**: One component of a wider portfolio of measures applied by individual countries, International Organisations or Regional Bodies to oppose, restrict and fight:

2.3.1 Aggression,

2.3.2 Terrorism,

2.3.3 Criminal behaviour or

2.3.4 Violations of human rights.

2.4 The intended purpose of such Sanctions (and other measures) is to:

2.4.1 Motivate a behaviour change on the part of the regime or jurisdiction concerned,

2.4.2 Deprive terrorists and criminals of access to funds.

3.0 LEGISLATION

3.1 HM Treasury is responsible for the implementation and administration of international financial sanctions in effect in the UK, for domestic designations under the Terrorist Asset-Freezing Act 2010, licensing exemptions to financial sanctions, and directions given under Schedule 7 to The Counter-Terrorism Act 2008. For up-to-date information on trade restrictions on exports refer to:

3.1.1 https://www.gov.uk/topic/business-enterprise/importing-exporting

3.2 Acuity has a legal duty to ensure its full compliance with all prevailing legal and regulatory requirements within the jurisdictions in which it operates.

3.3 It is essential for Acuity to manage its attention and compliance to sanctions and prohibitions in order to evidence and demonstrate the following:

3.3.1 Ensure an embargo on trading with specified countries/territories/regimes:
i.e. All such countries/territories/regimes as set out on the Company Sanctions List **(see Operational Procedure)**.

3.3.2 **Ensure ethical trading**
The purposeful refusal to trade with countries/territories/regimes in which state sponsored unethical/immoral practices exist.

3.3.3 Ensure non-support of Weapons of Mass Destruction programmes
Countries / territories / regimes of whom it is suspected that there is an active or intended WMD programme

3.4 Financial and Trade Sanctions (Sanctions) are one component of a wider portfolio of measures applied by individual countries, International Organisations or Regional Bodies to oppose, restrict and fight:

3.4.1 **Aggression**
The planning, preparation, initiation or execution by a person in a leadership position of an act of aggression.

3.4.2 **Terrorism**
The use of violence and intimidation in the pursuit of political aims.

3.4.3 **Criminal Behaviour**
Conduct of an offender that leads to and including the commission of an unlawful act.

3.4.4 **Violation of Human Rights**
Violation of the freedoms established by custom or international agreement that impose standards of conduct on all nations

3.4.5 **Money Laundering**
The process by which criminally obtained money or other assets (criminal property) are exchanged for 'clean' money or other assets with no obvious link to their criminal origins.

3.5 Nature of Goods

The following checklist outlines the broad categories of goods which are likely to be controlled:

3.5.1 Most items that have been special y designed or modified for military use and their components,

3.5.2 Dual-use items (i.e. those that can be used for civil or military purposes) which meet certain specified technical standards and some of their components,

3.5.3 Associated technology and software,

3.5.4 Goods that might be used for torture,

3.5.5 Radioactive sources.

3.6 The intended purpose of such Sanctions (and other measures) is to:

3.6.1 Motivate a behaviour change on the part of the regime or jurisdiction concerned,

3.6.2 Deprive terrorists and criminals of access to funds.

4.0 POLICY SCOPE

4.1 Absolutely without any exception, this Policy is mandatorily applicable throughout the entire Acuity business, together with all current and/or future potential 3rd Party outsourced functions and activities, including:

4.1.1 All direct employees of Acuity

4.1.2 Acuity ensure that this Sanctions Policy is complied with when giving work to:

4.1.2.1 Agency workers (i.e. temporary colleagues placed by recruitment agencies);

4.1.2.2 Self-employed 3rd Party Consultants and/or Contractors;

4.1.2.3 Any individual on work experience (including interns); and/or

4.1.2.4 Any individual training with the Group under a contract.

4.1.3 Compliance to this Policy Statement document is mandatory. There are no exceptions.

4.1.4 This Policy is held by the company and all Workers/Contractors are asked to familiarise themselves and acknowledge they have read and understood the policy.

4.1.5 It is the responsibility of all Workers/Contractors to:

4.1.5.1 Raise issues, questions and concerns in a timely manner,

4.1.5.2 Undertake follow up knowledge reinforcement as necessary,

4.1.5.3 Take all reasonable steps to ensure self-awareness of the requirements of the Policy Statement document and Acuity' position.

4.2 Controls (Risk Management)

Within the auspices of this Policy, Acuity hereby declares that it ensures the design, implementation and review of effective procedures, structures, systems and controls to

prevent breaches in sanctions management practices by any person acting on behalf of the company, and also has in place processes to identify such breaches.

4.3 Zero Tolerance

Acuity is committed to this policy, to the enforcement of The Act, and take a "zero tolerance" approach to any breaches in sanctions management practices by a member of staff. At staff induction, in periodic compliance training and in the Employee Handbook, Acuity clearly explains to all its staff that Acuity and/or its employees must never participate nor be engaged in the breaches of sanctions.

5.0 PENALTIES APPLICABLE AND ASSOCIATED FINANCIAL RISKS

5.1 The UK makes statutory instruments to provide for the penalties for any breach of EU sanctions and for the provision and use of information relating to the operation of those sanctions. The UK may also issue its own domestic financial sanctions and restrictions under the following pieces of legislation:

5.1.1 Terrorist Asset Freezing etc. Act 2010

5.1.2 Counter Terrorism Act 2008

5.1.3 Anti-Terrorism, Crime and Security Act 2001 and Counter Terrorism and Security Act 2015

5.2 Sanctions in the UK fall under the authority of several different departments:

5.2.1 The Foreign & Commonwealth Office (FCO) is responsible for negotiating international sanctions and has overall responsibility for the UK's policy on sanctions and embargoes.

5.2.2 HM Treasury (HMT) is the entity responsible for making designations under UK domestic financial sanctions and for the implementation and enforcement of all financial sanctions in the UK (through its subordinate agency, the Office of Financial Sanctions Implementation).

5.2.3 The Department of Business, Energy and Industrial Strategy implements some trade sanctions and embargoes.

6.0 EFFECTIVE SANCTION IMPLEMENTATION

6.1 The primary intention of Sanctions is for them to work. In so doing, having a meaningful impact and to act as a catalyst for behaviour change. To that end, Sanctions need to be applied in an effective and informed manner.

6.2 This Policy duly sets out to achieve that as follows:

6.2.1 The legitimate aims of the international community are achieved by applying sanctions in a timely and diligent manner;

6.2.2 Acuity does not engage in any attempts to frustrate or circumvent sanctions arrangements; and

6.2.3 Acuity' products and services are compliant with relevant legal requirements and

6.2.4 Acuity' products and services are delivered in a clear and transparent manner which lends itself to internal or external audit.

7.0 RISK RECOGNITION

7.1 Acuity maintains a Company Sanctions List of all countries / territories / regimes within its corresponding Operational Procedure. The primary point of reference for timely review and update being the HM Government Embargoes and Sanctions guidance:

7.1.1 https://www.gov.uk/browse/business/imports-exports/embargoes-and-sanctions

7.2 By default, this Company Sanctions List is the definitive benchmark of risk. Hence, any and all countries / territories / regimes listed thereon must be subject to Sanctions by all Acuity employees.

8.0 RISK PROFILING

8.1 With due acknowledgement to the recognition of risk within the context of Sanctions, Acuity commits to profiling its portfolio of individuals and companies with whom it becomes engaged in the legitimate course of its business.

9.0 CUSTOMER PROFILE: DEFINITION OF A BUSINESS RELATIONSHIP

9.1 A business relationship is defined as a business, professional or commercial relationship between a relevant person (that is, a business regulated under the Sanctions and Money Laundering Act 2017) and a customer, which is expected by the relevant person, at the time when contact is established, to have an element of duration

9.2 It is an arrangement between the business and the customer that anticipates an ongoing relationship between the two parties. This can be a formal or an informal arrangement. In general, it is for the business to decide what type of relationship it has with its customers, that is, whether they establish a business relationship or whether a customer is carrying out separate one-off transactions, even though they may be doing so on a regular basis.

9.3 However, the following circumstances would indicate that a business relationship exists:

9.3.1 A customer account is set up.

9.3.2 A loyalty card is issued.

9.3.3 Preferential rates or services are given.

9.3.4 Any other arrangement is put in place that facilitates an ongoing business relationship or repeated contact.

9.3.5 Source: HMRC Anti-money laundering guidance for trust or company service providers.

10.0 CUSTOMER PROFILING: PROFILING THE BUSINESS RELATIONSHIP PORTFOLIO

10.1 In understanding the Money Laundering risks associated with a client portfolio, Acuity takes diligent steps to understand the profile of its clients, the associated contractual status, and therefore has a stronger perspective from which to assess risk.

10.2 Most of Acuity's business relationships are the result of targeted sales approaches by Acuity and generate repeated transactions over the life cycle duration of a pre-determined period, as set out in a formal Contract.

10.3 However, some business relationships are the result of a client finding Acuity at the point of a specific business need. Such newly established relationships can be initiated through:

10.3.1 The client's own market research,

10.3.2 A recommendation of Acuity from another client,

10.3.3 Trade press advertising.

10.4 In these circumstances, the trading relationship commences prior to the formalisation of the relationship with a binding Contract between the Parties, and prior to meaningful interpersonal relationships have been established. Acuity recognises this as a risk and diligently records the status of such a relationship within Acuity' Client Relationship Management database.

11.0 PREVENTION: RISK BASED APPROACH

11.1 In order to focus on the key threats and vulnerabilities, and ensure effective risk management, Acuity has purposefully developed and deployed an approach which is **Risk based**.

11.2 In recognition that the nature of situation is an evolving one, Acuity appreciate that a process of ongoing review and evaluation is critical. To that end, this Policy Statement is subject to a formal review on an annual basis, thereby ensuring ongoing fitness for purpose.

11.3 Acuity maintains a Company Sanctions List of all countries/territories/regimes within its corresponding Operational Procedure. The primary point of reference for timely review and update being the HM Government Embargoes and Sanctions guidance:

11.3.1 https://www.gov.uk/browse/business/imports-exports/embargoes-and-sanctions

12.0 CONTROL: ACHIEVING POLICY OBJECTIVES

12.1 Acuity produces, invokes and trains its staff on this Policy in order that it delivers the following:

12.1.1 **Framework**:
Through clear, unequivocal guidance herein, provides a framework of requirements and accountabilities which are designed and intended to:

12.1.1.1 Ensure a consistent and effective approach to deter from non-compliance,

12.1.1.2 Ensure a consistent and effective approach to detect instances of non-compliance,

12.1.1.3 Disclose, as necessary, any trading practices to the relevant internal reporting lines and authorities.

12.1.2 **Explanation**:
Through clear, unequivocal guidance herein, provide the necessary explanation of:

12.1.2.1 The responsibilities of Acuity' employees in respect of the prevention, detection and, where appropriate, disclosure of trading activity by those acting on the Group's behalf.

12.1.3 Company Requirements:
Through clear, unequivocal guidance herein, sets out:

12.1.3.1 Acuity's mandatory requirements for the prevention and detection of trading practices including effective implementation of and monitoring compliance with this Policy.

12.1.4 Moral and Ethical Standards:
Supports the consistent achievement and culturally inbred expectation of high moral and ethical standards in all Acuity's business activities.

13.0 DRIVING COMPLIANCE AND MEETING OBJECTIVES: KEY ROLES AND RESPONSIBILITIES

13.1 For a Policy to be effectively implemented, the expectations and responsibilities of those required to implement it and be compliant to it must be set out.

13.2 Executive: Sponsorship and ownership
This policy requires that it is owned and sponsored at executive level by Anthony Flint; to whom ultimate responsibility for all aspects of its effective implementation falls.

13.3 Senior and Middle Management:
Awareness and Engagement:

13.3.1 All management are required to demonstrate absolute engagement with, and awareness of this Policy, its requirements, implications, penalties, consequences and systems and methods for data collection and reporting and evidencing compliance.

13.3.2 Managerial responsibilities as required by this Policy include, but are not limited to:

13.3.2.1 Proactively Driving
Awareness and engagement at all levels, including ensuring colleagues are aware that they must report any concerns via the processes specified in this Policy as appropriate and may do so without fear of recrimination.

13.3.2.2 Culturally Embedding
A 'business as usual' expectation of behaviours which are ethical and compliant to all Policy requirements.

13.3.2.3 Risk Based Documented Processes
Achieved through engagement and ownership of visible risk assessments, duly researching, evidential y deducing and formally documenting the level of risk exposure to trading across the Acuity business.

13.3.2.4 Control Processes and Procedures
Ensuring the effective design and implementation and effective

operational management to ensure minimisation of the risk of trading practices being undertaken within Acuity.

13.3.2.5 Executive Policy Owner Support
Provision of practical support and assistance to the Executive Owner of this Policy in the event of any trading activity being identified. Such support to include, as appropriate, liaison with external experts, law enforcement and regulators;

13.3.2.6 Customer Risk Assessment
Through intelligent and quantifiable analysis, understanding and documenting Acuity's potential susceptibility of its customer (including Politically Exposed Persons) to trading activity.

13.4 Employees (all levels)
It is everyone's responsibility to be ethical and diligent in ensuring that colleagues do not engage or assist in bribery or corrupt activities.

13.5 If any member of staff is identified to have been engaged in activities which are, or could reasonably have been construed, as being subject to sanctioned trading, gross misconduct based internal disciplinary action and consequences will follow.

14.0 STRUCTURE AND ORGANISATION

14.1 Acuity hereby commits to:

14.1.1 Ensuring, in supporting the effective implementation and ongoing compliance with the Policy, and management of sanctioned trading risks, that it deploys adequate and competent resource.

14.1.2 Ensuring, in supporting the effective implementation and ongoing compliance with the Policy, and management of sanctioned trading risks, that all areas of the business will be structured, organised and managed appropriately.

14.1.3 Such structure, organisation and management will include the provision of adequate senior management and visual and effective operational oversight both within the business unit and of internally or externally outsourced functions.

14.1.4 Ensuring the effective management of Sanction-related risks through:

14.1.4.1 The development and implementation of control systems.

14.1.4.2 Adequate and appropriately skilled resources are deployed to support said control systems.

15.0 RISK IDENTIFICATION

15.1 Acuity commits to ensuring the effective management of sanctioned trading risks through:

15.1.1 The development and implementation of control systems.

15.1.2 Adequate and appropriately skilled resources are deployed to support said control systems.

16.0 CHANGE MANAGEMENT AND COMPLIANCE SUPPORT MECHANISMS

16.1 Acuity commits to ensuring, in supporting the effective implementation and ongoing compliance with the Policy that suitably detailed training is undertaken.

16.2 All employee's will receive timely training, appropriate to the nature of their specific role in the effective implementation of this Policy, the prevention of risk, the identification of risk and/or non-compliance, the processes for reporting incidents if non-compliance and/or breaches, and the consequences of non-compliance and/or breaches.

16.3 An initial training programme will be followed up by the posting of the training session documents on the Training and development section of the staff intranet, and a schedule of refresher training at 12-monthly intervals. Line managers have responsibility to ensure that all employees within their team(s) are up to date with their training obligations in this, and other, respects.

16.4 Training to enable employees to recognise and deal with suspicious transactions includes:

16.4.1 The identity and responsibilities of the Nominated Officer (or MLRO).

16.4.2 The potential effect on the firm, its employees personally and its clients.

16.4.3 The risks of money laundering and terrorist financing that the business faces.

16.4.4 The vulnerabilities of the business's products and services.

16.4.5 The policies and procedures that have been put in place to reduce and manage the risks.

16.4.6 Customer due diligence measures, and, where relevant, procedures for monitoring customers' transactions.

16.4.7 How to recognise potential suspicious activity.

16.4.8 The procedures for making a report to the Nominated Officer.

16.4.9 The circumstances when consent is to be sought and the procedure to follow.

16.4.10 Reference to industry guidance and other sources of information

16.5 Acuity recognises that the production of this Policy Statement document is only the beginning.

16.6 The effective integration into day-to-day 'business as usual' will be largely dependent upon Change Management; i.e. the communication of its contents through a structured training programme in the form of group workshop sessions, delivered by a presenter accompanied by a set of Microsoft PowerPoint slides.

16.7 Acuity will ensure that relevant employees are made aware of their responsibilities under the Proceeds of Crime Act and the Terrorism Act to report knowledge or suspicion to the Nominated Officer and the requirements under the Sanctions and Money Laundering Act 2017 for the business to apply customer due diligence measures.

16.8 Annual testing of knowledge will be mandatory for all staff, with those identified as not having the required level of knowledge being scheduled for follow up training.

16.9 Decisions on the nature and level of detail of the training programme delivered to different levels and roles of employees will be risk based. The rationale of the associated due consideration of all other colleagues with the rationale for the document risk-based approach will be related to the roles and activities that employees undertake, e.g. more detailed training being given to:

16.9.1 Those who manage trading relationships with clients,

16.9.2 Those involved in business development,

16.9.3 Those involved in invoice payments (Accounts Payable)

16.10 All education and awareness activity will be diligently recorded by HR and shared with line managers in order to jointly evidence compliance, to generate management information, to identify any shortfalls and/or non-compliance with the training programme.

17.0 MEASUREMENT AND REPORTING

17.1 **Management Information:**
commits to ensuring that meaningful Management Information is produced and reviewed on a monthly basis by middle and senior managers. In order to assess compliance standards and highlight potential weaknesses such management information will include reports on compliance levels to appropriately developed and defined key risk and performance indicators. The development of these indicators must be with due diligence to the levels of relevance to the operating environment of the business area(s) concerned.

17.2 As reporting and knowledge through quantifiable information becomes mature, these indicators will be reviewed as required by the Policy executive owner in conjunction with senior managers. Such review being intended to focus on the completeness of available management information, the relevance of the indicators, the value that is derived from the reports, etc.

17.3 **Record Keeping:**
Acuity commits to ensuring that all areas of the business comply with the record keeping requirements of this Policy and that they are required to evidence record keeping compliance with this Policy.

17.4 Factors that are subject to mandatory record keeping include, but are not limited to:

17.4.1 Documentation of decisions taken and the rationale on which they are based;

17.4.2 Gifts and hospitality registers;

17.4.3 Whistleblowing records; and

17.4.4 Records of all Bribery and Corruption training undertaken.

18.0 CUSTOMER DUE DILLIGENCE: ACCEPTABLE ID AND SATISFACTORY VERIFICATION

18.1 Acuity recognises the importance of identifying and verifying the identity of the customer and any beneficial owner of the customer and obtaining information on the purpose and intended nature of the business relationship.

19.0 CUSTOMER DUE DILLIEGENCE: IDENTIFICATION (PRIVATE INDIVIDUALS)

19.1 Verification of the information obtained must be done using reliable and independent sources. These could be a document or documents provided by the customer, or data accessed electronically, or a combination of both. Where identification is done face-to-face, originals of any documents involved in the verification should be seen.

19.2 If documentary evidence of an individual's identity is to provide a high level of confidence it will typically have been issued by a government department or agency, or by a court, because there is a greater likelihood that the authorities will have checked the existence and characteristics of the person concerned. In cases where such documentary evidence of identity may not be available to an individual, other evidence of identity may give the business reasonable confidence in the customer's identity, although businesses should weigh these against the risks involved.

19.3 Non-government issued secondary documentary evidence of ID should only be accepted if it originates from a public sector body or another regulated financial services firm or is supplemented by knowledge that the business has of the person or entity, which it has documented.

19.4 If identity is to be verified from documents, this should be based on:

19.4.1 Either a government-issued document which incorporates:

19.4.2 The customer's full name and photograph, and

19.4.2.1 either their residential address,

19.4.2.2 or their date of birth.

19.4.3 Government-issued documents with a photograph include:

19.4.3.1 Valid passport.

19.4.3.2 Valid photo card driving licence (full or provisional).

19.4.3.3 National ID card (for non-UK nationals)

19.4.3.4 Firearms certificate or shotgun licence.

19.4.3.5 ID card issued by the Electoral Office for Northern Ireland.

19.4.3.6 Or a government issued document (without a photograph) which incorporates the customer's full name, supported by secondary evidence of ID, either government-issued or issued by a judicial authority, a public sector body or authority, a regulated utility company, or another FSA regulated firm in the UK financial services sector, or in a comparable jurisdiction, which incorporates:

19.4.3.6.1 The customers full name, and

19.4.3.6.2 either their residential address,

19.4.3.6.3 or their date of birth.

19.4.3.7 Government-issued documents without a photograph include:

19.4.3.7.1 Valid old-style full UK driving licence.

19.4.3.7.2 Recent evidence of entitlement to a state or local authority-funded benefit, tax credit, pension, educational or another grant.

19.4.3.8 Other documents include:

19.4.3.8.1 Instrument of a court appointment.

19.4.3.8.2 Current council tax demand letter or statement.

19.4.3.8.3 Current bank or credit/debit card statements (but not ones printed off the Internet).

19.4.3.8.4 Utility bills (but not ones printed off the Internet).

19.5 The examples of other documents are intended to support a customer's address, and so it is expected that they will have been delivered to the customer through the post, rather than being accessed by him from the Internet.

19.6 Where a member of Acuity staff has visited the customer at their home address, a record of this visit may constitute evidence corroborating that the individual lives at this address (that is, as a second document).

19.7 When accepting evidence of identity from a customer, it is important that the business makes sufficient checks on the evidence provided to satisfy them of the customer's identity and keeps a record of the checks made.

19.8 Checks on photo ID may include:

19.8.1 Visual likeness against the customer.

19.8.2 Does the date of birth on the evidence match the apparent age of the customer?

19.8.3 Is the ID valid?

19.8.4 Is the spelling of names the same as other documents provided by the customer?

19.8.5 Checks on secondary evidence of ID may include:

19.8.5.1 Do the addresses match the address given on the photo ID?

19.8.6 Dos the name of the customer match with the name on the photo ID?

19.9 Consideration should be given as to whether the documents relied upon may be forged. In addition, if a business chooses to accept documents that are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

19.10 Acuity staff must be vigilant, when accepting government issued documents, for forged or counterfeit documentation. Whilst there is no specific guidance on how to recognise genuine documents, the following indicators may assist businesses in identifying a document that may be false. Note this list is not exhaustive.

19.11 Fuzzy, unclear letters or numbers – in particular, the name, date of birth, expiry date on the presented ID.

19.11.1 Bumpy, rough or uneven surface texture over the information.

19.11.2 Tattered edges or any other evidence which might suggest the laminated surface has been tampered with.

19.11.3 Tattered or uneven edges around the photograph.

19.11.4 Lack of holographic, fine picture or watermark detail.

19.11.5 Does the information on the card match the details given to the business by the customer?

19.11.6 Has the documentation expired?

19.12 Any of the above could be indicators that the identity documentation presented may not be genuine. In this case, Acuity must make further enquiries on the customer and ask for further evidence of their identity. Where further documentation is provided Acuity staff should check for information consistencies.

19.13 The following table provides examples of documents that provide evidence of identity for some types of financially excluded customers. The list is not exhaustive. A proportionate and risk-based approach will be needed to determine whether the evidence available gives reasonable confidence as to the identity of a customer.

19.14

Customer	Documents
Economic migrants	• National passport, or • National Identity Card (nationals of EEA and Switzerland).
Refugees (those who are not on benefit)	• (Immigration Status Document with Residence Permit, or • IND travel document (that is, Blue Convention Travel Document, or • Red Stateless Persons document, or • Brown Certificate of Identity document).
Asylum seekers	IND Application Registration Card (ARC). **Note:** This document shows the status of the individual and does not confirm their identity.

20.0 CUSTOMER DUE DILLIGENCE: IDENTIFICATION (COMPANIES)

20.1 Standard Evidence:

To the extent consistent with the risk assessment carried out a business should ensure that it understands the company's legal form, structure and ownership. Acuity must obtain the following information as standard in relation to companies:

20.1.1 Full name

20.1.2 Registered number

20.1.3 Registered office in country of incorporation

20.1.4 Business address.

20.2 And, additionally, for private or unlisted companies:

20.2.1 Names of all directors.

20.2.2 Names of beneficial owners who hold or control over 25% of the shares or voting rights or otherwise exercise control over the management of the company.

20.3 Basic Verification:
Acuity must verify the identity of the corporate entity from:

20.3.1 Either a search of the relevant company registry, or

20.3.2 In the case of a publicly owned and limited company, confirmation of the company's listing on the regulated market, or

20.3.3 A copy of the company's certificate of incorporation.

20.4 The identity of any beneficial owners should be verified. Note the beneficial owner provisions do not apply to companies whose securities are listed on the regulated market.

20.4.1 For UK companies, a registry search will confirm that the company has not been, or is not in the process of being, dissolved, struck off or wound up.

20.4.2 For non-UK companies, similar search enquiries should be made through the registry in the country of incorporation.

20.5 Decisions on the extent of verification should consider the accessibility and reliability of information from jurisdictions.

20.6 Additional Verification to Address Identified Risk:
The standard evidence and basic verification requirements are likely to be enough to verify the identity of most corporate customers.

20.7 If, however, any of the circumstances relating to the customer, products, services or transactions are assessed to present a higher risk of money laundering or terrorist financing, then Acuity will need to decide what additional information must be obtained in order to be satisfied as to the customer's identity and to enable a thorough and effective risk assessment.

20.8 The verification processes for private companies, and for public companies that are not listed on the stock exchange or other regulated market, should consider the availability of public information on the company.

20.9 Verification may include, where appropriate, verifying the identity of one or more of the directors, the beneficial owners, or other representatives of the company by obtaining evidence of name, address and dates of birth in the same way as would be done for a private individual, for example, the production of a passport.

20.10 Acuity may also need to obtain additional information on the nature of the company's business, the reasons for seeking the product or service, and the source of funds. A visit to the customer's premises could be useful to verify the information provided on the company's business activities.

20.11 Simplified Due Diligence for Companies Listed on the Regulated Market: Businesses are not required to verify the identity of companies whose securities are listed on a regulated EEA market or equivalent overseas which is subject to specified disclosure obligations.

20.12 This exemption from the customer due diligence requirements is since these companies are publicly owned and generally accountable. The exemption also applies to companies that are majority-owned and consolidated subsidiaries of such companies.

20.13 If the regulated market is located within the EEA there is no requirement to undertake checks on the market itself.

21.0 BREACHES AND THE REPORTING OF BREACHES

21.1 All sanctioned trading risks or issues are to be reported immediately. Employees having a concern, or knowledge of, having suspicions of a violation of this policy are required to report the matter in a prompt and timely manner.

21.2 **Employee Reports:**
All bribery and/or corruption risks or issues are to be reported immediately. Employee's having a concern, or knowledge of, having suspicions of a violation of this policy are required to report the matter in a prompt and timely manner.

21.3 The first level of reporting should be to the individual employee's line manager. However, if the Party about whom the employee has concerns is that employee's line manager, the report should be made to the HR department.

21.4 Acuity Executive and Management Team recognises the obvious difficulties that any employee would be faced with in speaking up on such matters. It is the responsibility of al executives and managers to ensure that all employees are reassured that in doing so:

21.4.1 They are absolutely doing the right thing (for themselves and for the company),

21.4.2 That all information received will be treated seriously,

21.4.3 That all information will be investigated appropriately,

21.4.4 That if a breach of Policy is found to have taken place, the appropriate disciplinary measures will be entered with the person(s) who have been the perpetrator(s)

21.5 **Employee Reports:**
All sanctions risks or issues are to be reported immediately. Employee's having a concern, or knowledge of, having suspicions of a violation of this policy are required to report the matter in a prompt and timely manner.

21.6 The first level of reporting should be to the individual employee's line manager. However, if the Party about whom the employee has concerns is that employee's line manager, the report should be made to the HR department.

21.7 Acuity Executive and Management Team recognises the obvious difficulties that any employee would be faced with in speaking up on such matters. It is the responsibility of all executives and managers to ensure that all employees are reassured that in doing so:

21.7.1 They are absolutely doing the right thing (for themselves and for the company),

21.7.2 That all information received will be treated seriously,

21.7.3 That all information will be investigated appropriately,

21.7.4 That if bribery and corruption is found to have taken place, the appropriate disciplinary measures will be entered with the person(s) who have been the perpetrator(s)

21.8 Report Documentation:

If an employee requests to make a report of a suspected bribery and/or corruption incident, the report will be formally documented by the employee's line manager on the proforma on the next page.

APPENDIX 1: SUSPECTED SANCTIONED TRADING – REPORT TO LINE MANAGER / HR

Acuity Coaching Ltd – Suspected Sanctioned Trading – Report to Line Manager / HR	
From (Name):	
Department:	
Contact Details	
Email Address:	
Telephone Number:	
Details of Suspected Offence:	
On the reverse of this proforma, please set out the following:	
• Name(s) and address(es) of person(s) involved including relationship with Acuity. • Nature, value and timing of activity involved. • Nature of suspicions regarding such activity. • Provide details of any investigation undertaken to date. • Have you discussed you suspicions with anyone and if so on what basis? • Is any aspect of the transaction(s) outstanding and requiring consent to progress? • Any other relevant information that may be useful.	

This Policy has been approved & authorised by:

Name:	Simon Coops
Position:	Managing Director
Date:	12/02/2023
Signature: