X-Wrist
KYC Procedures and Policies

1. Introduction

1.1 The policy of NRG Core Global (X-Wrist) is to ensure that, by using a risk-based approach and a proportionate level of due diligence, we assess the potential money laundering and terrorist financing risk posed by each of our customers, in compliance with current legislative requirements and regulatory guidance.

1.2 The Company will use third party providers to carry out certain of the checks referred to below. In particular, we use Onfido to carry out:

1.2.1 Identity Document Checks (ensuring KYC documentation is not fraudulent);

1.2.2 Digital facial recognition; and

1.2.3 Checks to ensure that individuals are not subject to government sanctions, politically exposed persons (PEPs), and/otherwise present on or in adverse media lists and articles.

2. Procedures

2.1 X Wrist will assess the risk presented by each relevant customer, both at the commencement of the business relationship, and as the relationship develops. This assessment begins when a customer first registers and appropriate screening is immediately conducted.

2.2 X Wrist's compliance function, if necessary in liaison with the customer service team, are responsible for considering the risk posed by each new customer at the commencement of and throughout the business relationship. The Compliance Department collate data, research information and record the evaluation process. When complete, the information is uploaded to a central database.

2.3 Ongoing monitoring takes place so that the risk posed by a customer can be reassessed when circumstances change, or new information comes to light. Where necessary, approval of senior management will be obtained in order to continue engaging with a customer.

3. Review

3.1 The company will establish a Regulatory Compliance Committee to review decisions taken with respect to the business relationships that might create risk and review the suspension or cancellation of memberships as a result of AML non-compliance, adverse intelligence, insufficient source of funds/source of wealth information or suspicious activity.

3.2 Source of Funds (SOF) - refers to the origin of the funds involved in the business relationship. It refers to the activity that generated the funds, e.g. dividend payments from corporate ownership, salary payments, proceeds of a sale and the means through which the customer's funds were transferred.

3.3 Source of Wealth (SOW) - describes how a customer acquired their total wealth.

3.4 SOF and SOW will be relevant where Enhanced Due Diligence is necessary (please see further below).

4. Risk assessment process

4.1 Customer risk MUST be assessed at the commencement of the business relationship and continually reassessed by conducting ongoing monitoring of the relationship.

4.2 At the commencement of the business relationship the customer will be assessed by the Compliance Team. This dynamic assessment is based on an initial interaction with the customer; information provided by the customer; an initial screening that involves searching PEP/Sanctions lists and internal intelligence databases; and an internet search on information the customer has provided.

4.3 The level of risk applied to each customer is assessed through a number of key indicators such as:

4.3.1 the customer's business and wealth profile;

4.3.2 evidence of a legitimate source of funds;

4.3.3 the value of transactions/average level of spend;

4.3.4 countries associated with the customer (main residence and business trading);

4.3.5 method of buy-in;

4.3.6 international transfers;

4.3.7 PEP status; and

4.3.8 other information known about the customer.

5. Three stages of risk assessment

Stage 1

5.1 Initial risk assessment involves verifying identity at the commencement of the customer's membership. "Verifying" means establishing the customer's identity using information or documents obtained from a reliable source which is independent of the customer, such as official documents. Obtain details of residential and business addresses, all nationalities held by the customer, and occupation, including businesses and positions in those businesses, shareholding or other relevant information. Members must provide a physical residential and business address, rather than a "P.O. Box", "care of ' or "C/O" address for identification purposes. However, they may provide a P.O. or C/O address in addition for correspondence.

Stage 2

5.2 If the business relationship is identified as having any unusual elements, it is appropriate to look again at risk and to understand the customer's profile and/or the source of funds used in more detail. At this stage enhanced due diligence checks (EDD) are carried out and further risk assessment is undertaken regarding the business relationship.

Stage 3

5.3 Ongoing monitoring of the business relationship will take place where appropriate, Compliance will make decisions based on what is known about the customer and asks pertinent questions.

6. Customer risk

6.1 X Wrist has THREE levels of money laundering/terrorist financing risk: Low; Medium; and High.

6.2 Note that X Wrist cannot in any circumstances do business with a person appearing on a UK, EU or UN sanctions list including OFAC, HMT, Interpol, and UNSC. Any such sanctioned individual must be refused registration or ongoing subscription to our service. Their business relationship will be terminate d, their

account suspended and appropriate reports to HM Treasury and other relevant law enforcement agencies will be made.

6.3 An example of the profile for a Low, Medium and High-risk customer is shown below:

LOW RISK

Individual:

- Not a PEP.
- Not on a Sanctions List.

Country:

- Not domiciled in a sanctioned or high-risk country.

Transactional:

- Low spend profile.
- Main transactions are low level debit cards.
- No high-risk currency transactions noted.
- No poor credit history issues.

Level of due diligence required:

- Ensure we have recorded complete CDD details correctly in compliance with the MLR and Data Protection legislation.
- PEP and Sanctions screening process.
- Ensure that we have full name, residential and business addresses (not just a P.O. Box or C/O address), date of birth, occupation, all nationalities held.

MEDIUM RISK

Individual:

- A PEP with low level political contacts or in a low risk country.
- Not a PEP.
- Not on a Sanctions List.

Country:

- Not domicile in a sanctioned or high-risk country.

Transactional:

- Medium spend profile.
- International transfers from personal accounts in EU countries or other low risk countries.
- Other transactions are debit card.
- No high-risk currency transactions noted.
- No poor credit history issues.

Level of due diligence required:

Complete CDD, PEP and Sanctions screening process and Google search for adverse media. Ensure that we have:

- Full name, residential and business addresses (not just a P.O. Box or C/O address), date of birth, occupation, all nationalities held, and ethnic group.
- Appropriate scanned verification of identity documentation.
- Formal risk assessment is completed.

HIGH RISK

One or more of the following factors may result in the member being classified as Medium/High risk. If two or more of these factors are present, this is likely to result in the member presenting a higher risk of money laundering.

Individual:

- Higher risk PEP.
- Member from a high-risk country or with previous corruption or crime issues.
- On Sanctions List of another country (not UK/EU/UN) or is a possible hit.

Country:

- Place of birth, any residence or business is in a sanctioned or high-risk country.
- Transactional:
- High spend profile on buy in.
- Any international transfers from a high-risk country.
- Any high-risk currency transactions noted.
- Any poor credit history issues.

Level of due diligence required:

Complete CDD, EDD, PEP and Sanctions screening process and Google search for adverse media. Ensure that we have:

- Full name, residential and business addresses (not just a P.O. Box or C/O address), date of birth, occupation, all nationalities held, and ethnic group.
- Appropriate scanned verification of identity documentation.
- Formal risk assessment is completed.

7. Obtaining Due Diligence (CDD) and Enhanced Due Diligence (EDD) Information

7.1 If a customer refuses to provide details of their occupation/source of wealth (or where appropriate their source of funds) when they make an application to register, they must be advised that we are legally obliged to obtain this information during the course of or at the commencement of the business relationship. If a customer refuses to provide details of their occupation, source of wealth and/or source of funds, their customer profile must be noted accordingly and dated.

7.2 Failure by the customer to provide information requested will result in the business relationship being reviewed by the Compliance Team. This could result in moving the customer to a high-risk status and/or suspending or cancelling their membership.

7.3 When approaching a customer for personal and financial type information, discretion and sensitivity is necessary.

7.4 Where the individual has a significant and respectable public profile and information relating to their financial net worth is available without recourse to further investigation, it will be sufficient to document this in their profile with

reference to supporting electronic due diligence records, maintained by the Compliance Department.

7.5 Our third party provider (Onfido) will enable us to check all information provided and carry out the necessary checks. Open source Internet tools (Google etc.) may also be used to verify information provided by a customer.

7.6 Any high-risk customer who refuses to provide details of their occupation (or source of wealth/funds) must be advised that we are legally obliged to obtain this information. Failure to supply information may result in our deciding not to conduct business with the customer.

7.7 In assessing the potential risks posed by customers, we take into account all relevant factors, including:

7.7.1 the ease with which due diligence information has been provided and can be verified;

7.7.2 any potential country risks relating to the country where they reside or do business may need to be considered alongside overall risks during the business relationship (with reference to the Corruption Perceptions Index, Basel AML index and FATF list of high-risk and non-compliant countries);

7.7.3 the level of currency used;

7.7.4 suspicious activity; and

7.7.5 any information obtained from open sources; information provided by the customer personally or as a consequence of criminal activity or association or other regulatory sanction.

7.8 Customer Relations personnel are responsible for ongoing monitoring of the business relationship and to report any changes, e.g. increased levels of spend which might be considered to be unusual and not commensurate with what we know about the customer or a change in their occupation or awareness of business difficulties. Where changes are detected, the MLRO must be immediately informed.

8. Country risk

8.1 The Financial Action Task Force (FATF) and the Basel AML/CTF lists should, where customers are based outside the UK, also be referred to by the Compliance Department and included as part of their risk assessment.

8.2 The lists identify the countries that are subject to sanctions or otherwise regarded as non-co-operative in terms of AML/CTF compliance or are weak in certain areas. The Basel Index scores each country according to the risk rating assessed by the Basel Institute on Governance. The Finance team are immediately informed about changes in respect of any country to assist them maintain vigilance and identify transaction s originating from locations which are high risk.

8.3 Member States of the European Economic Area (EEA) can generally be presumed to be low risk, since like the UK they are subject to the Fourth EU Money Laundering Directive. However, standards of implementation of the Money Laundering Directive may vary across Member States, therefore the Compliance Department will regard any country specific information indicating a higher risk posed by an EEA country.

July 2019 (Ref APH)