ANTI-MONEY LAUNDERING GUIDE

Ethics & Compliance Office

April 2025

Classification: **External**

Contents

1. INTRODUCTION

This document provides guidance on the application of the Finance Standards and the Vivo Energy Code of Conduct in the areas of anti-money laundering ("AML") and combating terrorist financing. The Vivo Energy Code of Conduct covers principles relating to Money Laundering that all staff must follow. This document explains how Vivo Energy Business Units can act to assess their exposure to money laundering risks and how to establish adequate controls to enable staff to comply with these principles.

Anti-money laundering provisions in general are designed to deter criminals from making use of legitimate businesses for the purpose of financial crime or injecting illegitimate cash back into legitimate businesses, and to assist law enforcement agencies to trace and recover criminal assets and terrorist funding.

They include making the proper enquiries about the origin of monies and property received or procured and the appropriateness of the destination of money forwarded in transactions. Some of the relevant compliance steps, such as the Denied Party Screening checks, are also required for Trade Controls and Anti-Bribery and Corruption compliance.

Primary responsibility for implementing and maintaining effective AML controls and reporting on suspicious activities rests with the relevant Vivo Energy Business or Function.

This AML Guide does not attempt to supersede measures already taken by certain Vivo Energy Business Units to implement anti money laundering procedures and controls but rather establishes principles based guidance for all Business Units in Vivo Energy to ensure Group wide coverage of common requirements across various jurisdictions. Any additional applicable local laws and regulations must also be complied with.

The Chief Legal and Compliance Officer is the custodian of this Guide.

For the purpose of simplification, the Guide will refer to anti-money laundering only but takes into account requirements relating to combating terrorist financing.

2. MONEY LAUNDERING AND THE LAW

'Money laundering' is a generic term used to describe the process of hiding the criminal origins of money or money's worth (the 'proceeds of crime') within legitimate businesses or business activities. The term also describes the use of money of legitimate origin to support terrorism.

Preventing money laundering and terrorist financing activity is a global concern. A number of supranational organisations have been established to deal with these issues and by far the most important and influential of these bodies is the Financial Action Task Force ("FATF"). The FATF is an intergovernmental body whose purpose is to establish international standards and develop and promote policies, both at national and international levels, to combat money laundering and the financing of terrorism.

Many of the countries where Vivo Energy operates now have some form of anti-money laundering legislation. The legislation tends to place criminal liability on both the company and its employees. Penalties for money laundering can be severe. In the United States and the United Kingdom, for instance, individuals convicted of money laundering face imprisonment for each money laundering offence. Businesses face fines which may amount to millions of US dollars. Any property involved in the transaction or traceable to the proceeds of the criminal activity, including loan collateral, personal property, and, under certain conditions, entire bank accounts (even if some of the money in the account is legitimate) may be subject to forfeiture.

The main money laundering risk for Vivo Energy is that it unwittingly becomes involved in money laundering activities through its dealings with unknown (i.e. not properly screened) counterparties or it fails to report or monitor a suspected or actual money laundering incident.

The offences covered by anti-money laundering provisions include:

1. Money laundering: Acquiring, using or possessing criminal property; concealing the nature, source, location or ownership of criminal property; converting or transferring criminal property or removing it from a country; use or control of criminal property; and assisting terrorist financing in any other way.
2. Tipping-off: Disclosing (in particular to the subject) anything likely to prejudice an investigation.
3. Prejudicing an investigation: Falsifying, concealing, destroying or disposing of relevant documents.
4. Failure to report: Not reporting a suspicion when there are reasonable grounds to know or suspect that someone is laundering money.

3. RISK BASED APPROACH

Legislators encourage companies to take a risk based approach in managing the money laundering risk generally and in developing and operating AML controls (e.g. applying counterparty due diligence measures). In line with this, Vivo Energy applies a risk based approach in devising controls and procedures to deal with the risk of non-compliance with external AML requirements.

Key elements include:

1. Fit for purpose Know your Counterparty (KYC) screening.
2. Monitoring of high risk counterparties and related transactions.
3. Central reporting of unusual or suspicious transactions.
4. Record keeping in relation to business transactions and reports on money laundering suspicions.
5. Training of staff.

All Businesses and Functions are expected to address these elements as set out below.

This also applies to Joint Ventures where Vivo Energy has a controlling interest or is the operator.

4. COUNTERPARTY DUE DILIGENCE

Know your Counterparty (KYC) screening allows Business Units to assess the exposure of the counterparty to a range of risks. One of the key requirements of AML legislation is the need to know our counterparties. Vivo Energy should never establish a business relationship with a counterparty until we are reasonably satisfied with the level of knowledge of the counterparty's true identity. All counterparts should be screened in accordance with the Vivo Energy KYC Policy.

In consequence a standard control should be implemented to only open an account for a new counterparty in the relevant Vivo Energy systems (e.g. SAP Winshuttle, etc.) following completion of the required KYC as well as the Workflow checklist.

The KYC screening process described below sets out the suggested approach to meet principal AML requirements. The described KYC requirements do not apply to low value transactions in relation to AML requirements. Low value transactions mean a single or a series of related transactions below **USD 10,000.**

4.1 Timing of Counterparty Identification and Verification

KYC should be concluded before a new business relationship is established (i.e. before any contract signing or binding commitment takes place).

Verifying a counterparty's identity and ownership generally only applies to new counterparties. However, if there is any doubt as to an existing counterparty's identity or true ownership (due to changing circumstances), the KYC process should be repeated.

4.2 Counterparty Risk Classification:

New counterparties entering into a business relationship with Vivo Energy or conducting one-off transactions as principal or agent for someone else should be classified in terms of the potential money laundering risk (i.e. high, medium or low risk).

This counterparty risk classification will be performed against the following risk dimensions:

4.2.1 Geographical risk

Assessing the geographical risk means to consider the jurisdiction in which the counterparty is operating and how that jurisdiction is judged both externally and internally with regard to fraud, corruption and other financial crime. This will depend largely on how the country has applied international standards to combat financial crime.

4.2.2 Counterparty risk

Contributing factors to the counterparty nature and thus the counterparty risk will include the type of firm and its place in the market place, whether it is regulated, the transparency of its ownership and whether it has a listing on an acceptable stock exchange. A regulated company or well-known oil major is likely to be seen as low risk while a private company with complex/obscure ownership or which is registered in one country but trades from another would be seen as higher risk. Also new market players may pose a higher risk to us than longstanding relationships with well-known market participants. Strong efforts to address this factor will also assist Vivo Energy Business Units in avoiding bribery and corruption risks.

Guidance regarding geographical and counterparty risk can be obtained from the VE Ethics and Compliance Office

4.3 Due Diligence Documentation Requirements:

KYC LEVEL	COMPANY DOCUMENTATION AND DUE DILIGENCE REQUIREMENTS
Simplified for low and medium risk counterparts	1. Full name 2. Registered number 3. Registered name and address and business address

KYC LEVEL	COMPANY DOCUMENTATION AND DUE DILIGENCE REQUIREMENTS
	4. Nature of the counterparty's business and of the envisaged transaction Plus (as applicable): 1. Completed VE Supplier/Customer registration form (Outline of the anticipated business) 2. Company Registration Document (Company registry or certificate of incorporation or third party verification) 3. Bank letters. For individuals: The minimum information required is the true name, address & date of birth evidenced by a form of ID recognised in the jurisdiction
Standard for low and medium risk counterparts above USD 50K transactions	Simplified KYC plus: 1. A list of current directors (names) of the company 2. Names of all individual beneficial owners with holdings of 25% or more and in any case the beneficial owner with operational control, and if owned by a corporate entity, a list of ultimate beneficial owners, shareholders etc. 3. Identification of involvement of any Political Exposed Persons ("PEPs"). For actions to be taken in case of a PEP involved refer to the section below.
Enhanced for JV's and acquisitions and high risk counterparts etc.	Standard KYC plus: 1. Latest company report and statutory accounts. Additional information to help verify the identity of the counterparty: 1. How well are the owners/directors/managers known to Vivo Energy? 2. Visit to the place of business to verify address and operations. 3. Verification of the names of beneficial owners as defined for Standard KYC above. 4. Verify the ID of individual directors (and possibly shareholders)

4.3.1 Denied & Restricted Party Screening - People Or Entities With Whom Vivo Energy May Not Deal

Economic, trade or financial sanctions are imposed by governments or the United Nations to exert pressure on individuals or political regimes and for the advancement of foreign policy objectives. Sanctions include a range of financial or trading restrictions, such as freezes on the assets of and travel restrictions on nominated individuals, bans on financing of state-owned enterprises, prohibitions on the supply of technical, financial and other assistance and outright prohibitions on trade.

In order to make sure that Vivo Energy does not deal with any denied counterparties (and thus avoid committing a criminal offence), Business Units principally need to ensure that they screen their counterparties in accordance with the Vivo Energy KYC policy.

4.3.2 Political Exposed Persons

Where a PEP has been identified as being a beneficial owner holding or controlling 25% or more of the voting rights of a counterparty, that counterparty must be treated as high risk and the Enhanced KYC measures applied. In such circumstances the identity of the individual must be verified and consideration should be given as to whether the requirements of the Vivo Energy Government Anti-corruption Manual also apply.

5. MONITORING OF COUNTERPARTY TRANSACTIONS

AML regulations require conducting ongoing monitoring throughout the business relationship with a third party with the objective of:

1. Scrutinising transactions to ensure they are consistent with the counterparty's knowledge and the purpose of the business relationship.
2. Ensuring that documentation and information held about the counterparty is kept up to date.
3. Identifying abnormal transactions and/or activities for further examination and allowing reports to be made and reviewed promptly by the right person(s).
4. Supporting appropriate action on the findings of any further examination.

Vivo Energy, Business Units should introduce a standard control to perform counterparty reviews. The reviews should be performed at least at every contract renewal stage and includes the

following:

1. Check if there have been any changes to the counterparty's management or control (request details from counterparty)
2. Accuracy of the identification information on file (including banking and payment details)
3. Repeat Denied Parties screening (sanctions check).

If concerns cannot be resolved the matter should be discussed with the local Finance Manager and CLCO and, if it is decided that the activity or circumstances amount to suspicion, a report must be submitted as set out in Section 7 below.

6. ADDITIONAL CONTROLS TO MITIGATE MONEY LAUNDERING EXPOSURE

In relation to AML certain additional controls are recommended as best practice:

1. Acceptable transaction settlement procedures should be agreed with counterparties upfront (this includes the use of acceptable banks and accounts, payments on behalf of the contract counterparty and repayment procedures for rebates).
2. All transactions should be automated and the use of manual, paper, cash or cheque for payments or receipts should be restricted.
3. Refunds will always have to flow back to the counterparty via a credit note or bank transfer from whom funds have been received and to the tax jurisdiction from where the funds have been paid. Refunds may only be processed if the required documentation as per the Vivo Energy Workflow checklist has been verified.
4. As general guidance we should not accept cash settlements (there is no minimum materiality limit for this), money orders, travellers cheques or cheques drawn on accounts in the name of third parties (i.e. payments drawn on accounts in the name of someone other than the invoiced customer who made the purchase)
5. If cash or cheque payments or receipts are required (e.g. as legally obliged in certain jurisdictions), additional controls should be implemented (especially when cash amounts will exceed the equivalent of USD 10,000 in connection with a single sales transaction or a series of related sales transactions);
6. Order, shipping and invoice documentation should quote counterparty data as it appears on our system.
7. Bank details should be confirmed in accordance with the Vivo Energy Workflow Checklist and all exceptions must be referred to the Ethics and Compliance Office for approval.

Following the introduction of the above suggested controls and procedures, Business Units would be in a robust position to avoid becoming a victim of money laundering activities. Business Units

may nevertheless have to consider abandoning individual transactions or whole business relationships upon identification of high-risk counterparties and identifying concerns that cannot be resolved.

Applicable law in various countries may also require the reporting of the receipt of currency as payment. For example, the US requires reporting to the IRS of the receipt of currency and currency equivalents (such as travellers' cheques) totalling more than USD 10,000 in a single or a series of related transactions.

7. RECOGNISING AND REPORTING SUSPICIOUS ACTIVITIES

Each employee is required to report when he/she, by him/her selves or following consultation with others, conclude that he/she "knows or suspects, or has reasons to know or suspect that a person or counterparty is engaged in money laundering or terrorist financing. Failure to comply may result in a criminal offence by the company and for individuals who may face imprisonment as well as disciplinary action. There is also no minimum threshold for this reporting requirement, i.e. all suspicions regardless of the value involved need to be reported.

7.1 When to Report

To avoid any conflicts, staff members need to be able to show that they took all reasonable steps in the particular circumstances to know the counterparty and the reason for the transaction. This in practice means following identification procedures properly and making sure that identified Red Flags are followed up and resolved.

An issue in relation to potential money laundering will often start with a concern relating to a Vivo Energy counterparty, either because our KYC screening activities cannot generate the information we need to clear the counterparty, or the outcome is concerning or because we detect unusual behaviours or transaction patterns with one of our existing business partners, i.e. there are Red Flags that need to be resolved.

In such a case the situation should be discussed internally with the local Finance Manager or Chief Legal and Compliance Officer to decide the way forward. A note of this should always be recorded and retained. In the case of a real suspicion of actual or attempted money laundering, this suspicion must be reported to the Vivo Energy Global Helpline. No time must be wasted as applicable regulatory requirements may require immediate reporting.

Staff also need to be reminded that it may be an offence to tip off a counterparty or an individual suspected of money laundering (i.e. release any information which is likely to alert the subject to the fact that a report has been made or which is likely to prejudice an investigation). For this reason all reports must be treated confidentially. Regardless of whether the decision is then made to report the suspicion internally or not, retention of all records is required for audit purposes.

7.2 How to Report

All cases of money laundering (knowledge about an incident or suspected case) must be reported internally via the Vivo Energy Global Helpline. This way staff will have discharged their duty to report their suspicion of money laundering activities and the Internal Audit Department will work together with CLCO and other relevant experts to determine necessary next steps. These steps may include:

1. Acknowledgement of the receipt of the report and providing a reminder of the requirement for the reporting Business Unit to do nothing that might prejudice an investigation or tip off the counterparty
2. Requesting additional information from the Business Unit if deemed necessary and forwarding these information to the relevant Country Finance Manager and CLCO in the jurisdiction to which the incident relates.
3. The Country Finance Manager will decide on the basis of the available evidence and other relevant information, whether to file an external report. Such Suspicious Activity Report ("SAR") will be passed to the relevant external authorities and subsequently support be provided to any potential investigations.
4. Applying for consent to proceed with a planned transaction from the relevant external, local authorities if so required (necessary for certain jurisdictions).
5. Responding to the Business Unit on whether a specific, proposed transaction can go ahead. This may be conditional on approval from external authorities if an external report has been filed.

8. RECORD KEEPING

It is important to retain adequate counterparty and transactional records as regulators or law enforcement agencies may request to look at these as part of an investigation. The records will provide an audit trail and need to be easily retrievable. Failure to meet external record requirements can be a criminal offence. In principle the applicable Group Records Management procedures of the Business or Function must be followed. Acceptable records are original documents, photocopies of originals and scanned or electronic records. File retention periods may need to be adjusted to meet general AML requirements as set out below.

8.1 Types of Records to Be Retained

1. **Client information:**
   Records of KYC including investigation and resolution of Red Flag situations are to be retained for a period of at least 10 years after the account or the relationship ends.

2. **Transactions:**
   It is of importance to follow existing records management requirements for transaction records retention to also support AML record keeping requirements.

3. **Internal and external reports.**
   A record of all internal and external reports relating to suspicions on money laundering activities, together with associated correspondence and supporting evidence will be retained by the Internal Audit Department. Also records of actions taken following the internal and external reporting procedures (including copies of all Suspicious Activity Reports) must be retained for 10 years after the report was made.

4. **Reports made by the Internal Audit Department:**
   These reports to senior management and all action taken as a consequence are also to be retained.

5. **Training and compliance monitoring:**
   Records of training delivered including the date the training was delivered, the nature of the training and the names of the staff trained are all held on file and the records retained for a minimum of 5 years.

9. TRAINING OF STAFF

Regular training ensures staff stay aware of their responsibilities in respect of prevention of money laundering including the application of adequate controls, understanding what might constitute suspicious behaviour and how to report any such suspicions. It is important to ensure that training is delivered on a timely basis, as failure to train a staff member may leave the company open to prosecution or regulatory sanction.

Training will be delivered to all Vivo Energy staff in line with the yearly Vivo Energy training schedule.