ANTI MONEY LAUNDERING POLICY

ANTI-MONEY LAUNDERING POLICY

CONTENTS PAGE

PART 1: KEY UPDATES AND POINTS OF SIGNIFICANCE[1]

1. POLICY UPDATES

1.1 Emphasis on the risk of committing AML offences by dealing in the "proceeds of crime", even if there is no intention to "launder" those proceeds.

1.2 References to "trade-based" money laundering, which has grown in significance in recent years.

1.3 Emphasis on importance of escalating red flags during the course of a relationship with a counterparty. AML risks continue beyond on-boarding and require ongoing review, assessment and management.

1.4 Reference to employees needing to be mindful about the risk of prejudicing investigations when they raise money laundering concerns.

---

2. PRACTICAL / PROCEDURAL IMPLICATIONS

2.1 Compliance risk assessments should cover the risk of the business dealing in the "proceeds of crime". Section 3.3 and 3.4 of the Policy highlight four particular risks to consider.

2.2 Consider whether there are any other relevant risks, based on the nature and geographical locations of your business's operations.

2.3 AML policies/procedures should reflect this policy and should also be reviewed in light of the abovementioned risk assessment to ensure that they address the specific risks that the business faces.

---

3. TRAINING

3.1 A risk assessment should be conducted to determine which employees are more exposed to money laundering risk. This could include, for example: employees in finance who check payments against contracts; or employees involved in corporate or commercial activities in higher risk countries where there is a greater risk of contracts being obtained through corruption. Senior management should also be made aware of

[1] Please note this is a non-exhaustive summary. The full policy should be reviewed and assessed for further training, practical and procedural implications and updates that are specific to your business.

money laundering risks.

3.2 Employee training materials: (i) discuss the risks identified in the risk assessment; and (ii) reflect the Melrose Anti-Money Laundering Policy and where relevant any consequent revisions to any local AML Policy. In particular, employees should: understand the broad scope of money laundering law (including any local laws as applicable); absorb the expanded list of red flags in section 5.1 of the Melrose Anti-Money Laundering Policy; be reminded of the importance of being alert to red flags during the course of a relationship with a counterparty, per section 5; and be alerted to risk of making disclosures that could prejudice investigations, per section 5.2.

PART 2: ANTI-MONEY LAUNDERING POLICY

1. POLICY STATEMENT AND OBJECTIVES

1.1 Melrose Industries PLC and its business units (collectively referred to as the **"Group"**) are committed to preventing money laundering. The Group and its employees can commit offences by dealing in the proceeds of any person's crime, and we take seriously the responsibility of ensuring our business is not used for the purposes of money laundering and are committed to best practice in this area.

1.2 The purpose of this policy is to establish the framework that the Group will follow in order to avoid dealing in the proceeds of crime, to support law enforcement authorities' activities to detect the proceeds of crime, and to help prevent laundering of the proceeds of crime.

1.3 The Group requires all employees of the Group and its business units to adhere to this policy in order to prevent the use of our Group and its products and services being used for the purposes of money laundering. Adherence to the policy is critical to ensure that all business units in the Group, regardless of geographical location, comply with our obligations in respect of preventing money laundering.

1.4 This policy complements the Anti-Bribery and Corruption, Trade Compliance, Whistleblowing and Document Retention Policies. Your business unit may have a specific process or policy in addition to this policy which you will need to follow.

---

2. MAINTENANCE OF THIS POLICY

2.1 This policy has been approved by the board of directors of Melrose Industries PLC, who are responsible for ensuring this policy complies with relevant legal and ethical obligations.

2.2 The General Counsel for each business within the Group is responsible for ensuring awareness of and compliance with this policy within their particular business unit.

2.3 Each business within the Group is expected to establish a "culture" of compliance with this policy. The executive team of each business must take direct responsibility for ensuring effective transmission of this policy throughout their business unit, together with relevant guidance and training, and appropriate safeguards, monitoring, and resources, in order to ensure compliance with this policy.

3. BACKGROUND

3.1 Money laundering is the process by which the proceeds of crime are converted into assets which appear to have a legitimate origin, so that they can be retained permanently, or recycled to fund further crime. The "proceeds of crime" are, broadly speaking, money or other property which results from any criminal conduct, including (for example) bribery and corruption, tax evasion, modern slavery and breaches of competition law.

3.2 Money laundering is the process by which the proceeds of crime are converted into assets which appear to have a legitimate origin, so that they can be retained permanently, or recycled to fund further crime. The "proceeds of crime" are, broadly speaking, money or other property which results from any criminal conduct, including (for example) bribery and corruption, tax evasion, modern slavery and breaches of competition law.

3.2.1 Placement - Placement is the process of placing criminal property into the financial system. It might be done by breaking up large sums of cash into smaller amounts or by using a series of financial instruments (such as cheques or money orders) deposited at different locations.

3.2.2 Layering - Layering is the process of moving money that has been placed in the financial system in order to obscure its criminal origin. It is usually achieved through multiple complex transactions often involving complicated offshore company structures and trusts.

3.2.3 Integration - Once the origin of the money is disguised it ultimately must reappear in the financial system as legitimate funds. This process involves investing the money in legitimate businesses and other investments such as property purchases or setting up trusts.

3.3 Given the nature of the Group's activities, a key money laundering risk for the Group is "trade-based money laundering". This is the use of trade transactions to disguise the origins of criminal proceeds, for example by over- or under-invoicing goods and services, or over- and under-shipments of goods and services.

3.4 Given the nature of the Group's activities, a key money laundering risk for the Group is "trade-based money laundering". This is the use of trade transactions to disguise the origins of criminal proceeds, for example by over- or under-invoicing goods and services, or over- and under-shipments of goods and services.

4. COUNTERPARTY DUE DILIGENCE

4.1 As part of our commitment to prevent money laundering, the Group must ensure that it completes adequate counterparty due diligence on all of its customers, vendors, and other counterparties to reduce the risk of the Group dealing in the proceeds of crime or being used by a counterparty who wishes to launder money.

4.2 The counterparty due diligence process that must be followed is:

4.2.1 Ascertainment of Counterparty Identity

- The counterparty's identity should be verified on the basis of documents, data or information obtained from a reliable and independent source, e.g. checking with the organisation's website to confirm the business address, checking the governmental registry of companies in the country in which the counterparty is based;

4.2.2 Establishment of Ultimate Beneficiary

- The beneficial owner(s) of the counterparty should be identified. The beneficial owner is the natural person who either ultimately controls the counterparty, or directly or indirectly owns more than 25% of the counterparty[2].

- You should also consider whether there is any other person on whose behalf or for whose benefit a transaction or activity is being conducted, if not the counterparty, and if so, identify their beneficial owner(s).

4.2.3 Establishment of the purpose of the business relationship

- If the counterparty is a new one, the rationale for wanting to transact with us should be established.

- You should also ask the counterparty to explain the reason for the transaction in question and, in this context, you should pay attention to the "red flags" set out in section 5 below.

4.2.4 Potential Sanctions Issues

- If a counterparty is located in a jurisdiction subject to

[2] For UK-registered companies, such information is often available on the Companies House website. Other jurisdictions may also have public registers of beneficial ownership.

sanctions, additional due diligence must be completed in accordance with the Trade Compliance policy.

- You should bear in mind that individuals, companies and specific assets (e.g. aircraft, ships), can be subject to sanctions. If you have any concerns these may apply, you should report such concerns to the General Counsel of your business unit.

---

5. REPORTING REQUIREMENTS – RED FLAGS

5.1 The following circumstances should be seen as "red flags" in relation to the risk of the Group dealing in the proceeds of crime or being used for the purposes of money laundering. You should report any of the below, or any wider concerns you may have in relation to a transaction/contract, to your General Counsel for purposes of determining whether enhanced due diligence and/or making appropriate confidential notification(s) to the relevant authority / authorities is warranted.

5.1.1 A counterparty provides minimal, vague or fictitious information about itself or the reasons for wanting to do business.

5.1.2. A counterparty is overly secret or evasive about its ultimate beneficial owner.

5.1.3. The counterparty's proposed business activity is inconsistent with its wider business profile.

5.1.4 A counterparty provides false or counterfeited documentation.

5.1.5. A counterparty is using an agent or intermediary without good reason.

5.1.6. A counterparty is actively avoiding personal contact without good reason.

5.1.7 A counterparty wishes to pay or receive payment in cash. Cash receipts from counterparties and cash payments should be actively discouraged. No payment to the Group will be accepted in cash if it exceeds £1,000. Cash payments made by the Group are only authorised where they amount to less than £1000. An exception to this may be made in specified circumstances in relation to cash advances to employees. In such cases the Group Policy on cash advances to employees must be followed.

5.1.8 A counterparty is based in a country where there is a higher risk of criminality or money laundering, such as a High Risk Country

under the Trade Compliance Policy.

5.1.9. The counterparty is the subject of allegations of criminal conduct.

5.1.10. The counterparty requests payments to or from a third party, or country other than the country where it is incorporated or where the transaction is based.

5.1.11. A counterparty makes an overpayment requiring a refund.

5.1.12. There are significant discrepancies between a counterparty's invoices, shipments and contract with the Group.

5.2 When raising concerns, Group employees should be mindful about making any communications that could prejudice investigations by law enforcement authorities, contrary to applicable law.

6. TRAINING

6.1 All Group employees in a sales, procurement, compliance or legal role, and any other relevant personnel as determined by the appropriate General Counsel for each business unit, are required to complete anti-money laundering training. This training should cover, at a minimum, the meaning of anti-money laundering requirements and the risks of non-compliance.

6.2 The training must be completed every 18 months.

The appropriate General Counsel for each business unit within the Group is responsible for ensuring participation in this training and for maintaining documentation of the training.

PART 3: KEY TRENDS AND DEVELOPMENTS

Money laundering enforcement is on the increase in Europe, and is a focus of law enforcement authorities in the UK. A key risk for companies outside the regulated sector is "trade-based money laundering". This factsheet outlines some key trends and developments in this risk area.

- **AML enforcement and penalties are increasing.**

According to public sources[3], there were 58 AML penalties in 2019 totalling US$8.14 billion, compared to 29 penalties totalling US$4.27 billion in 2018. Although historically the US has been the most active enforcer, enforcement in Europe is increasing: in 2019, European AML penalties totalled US$5.8 billion, exceeding US penalties of US$2.2 billion. In the UK, the National Crime Agency (NCA) estimates that hundreds of billions of pounds may be laundered through the UK annually[4]. In recent years, the UK has strengthened the powers of law enforcement agencies to deal with money laundering. For example, in 2018 Unexplained Wealth Orders were introduced, which require a person to explain how they obtained certain property. In addition, where corporates are investigated for criminality, the authorities may including money laundering charges: for example, in May 2017 the UK Serious Fraud Office announced that it is investigating Petrofac PLC suspected bribery, corruption and money laundering.

Although there is a particular focus on money laundering in the regulated sector, non-regulated companies can also commit money laundering offences if they deal in the proceeds of crime. For example, if a company obtains a contract through bribery, the proceeds of the contract will constitute the proceeds of crime. Similarly, any benefit that a company may obtain through other forms of corporate criminality, such as modern slavery or anti-competitive conduct, will constitute the proceeds of crime. A company which then deals in the proceeds of crime, for example by receiving the proceeds of a corrupt contract, may commit laundering offences – even if the company is not seeking to "launder" those proceeds in the sense typically understood.

Where a company suspects that it may have engaged in conduct that could have given rise to proceeds of crime, it should carefully consider whether a report ought to made to the authorities. In the UK for example, it is possible to seek consent from the NCA in order to deal with the proceeds of crime. The company should also bear in mind that its auditors may have independent obligations to report suspected money laundering to the authorities, as in the UK.

- **"Trade-based money laundering" is a particular risk to trading companies.**

"Trade-based money laundering" (TBML) is the use of trade transactions to disguise the origins of criminal proceeds. For example, a supplier could over-invoice goods or describe them as higher quality (and therefore higher value) than they really are, so that the customer effectively transfers additional value to the supplier in the form of an excess payment. A recent report from the US General Accountability Office indicates that, in the US at least, TBML may be increasing partly because of US financial institutions' improved compliance with AML regulations[5]. In the UK, the NCA

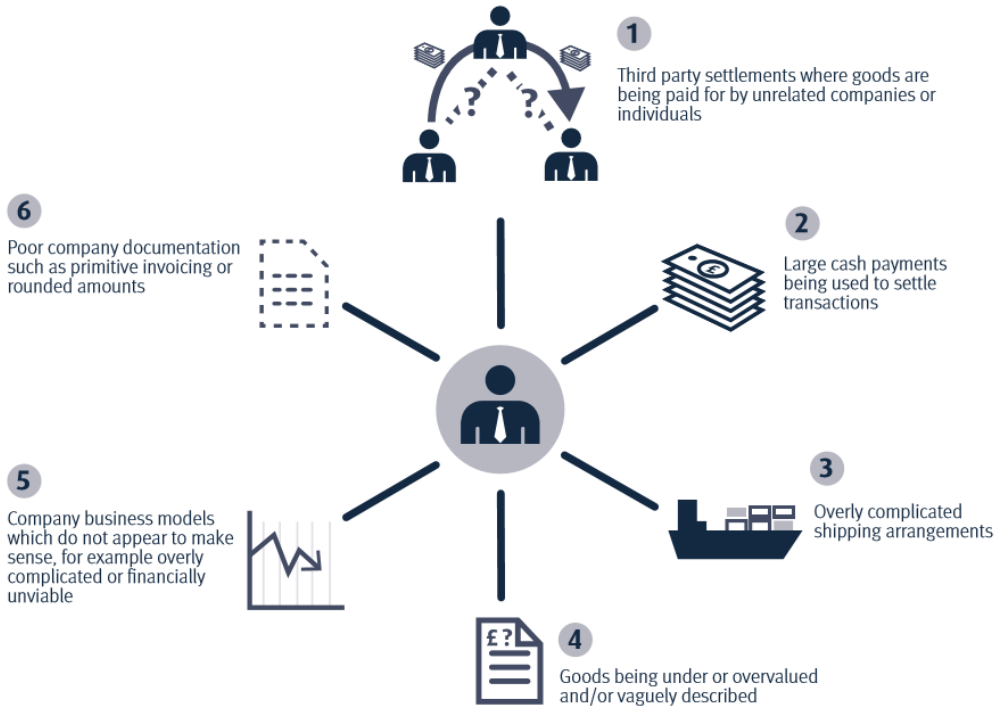
3 *Anti-Money Laundering Trends and Challenges*, Global Investigations Review, 1 June 2020.

4 *National Strategic Assessment of Serious Organised Crime 2020*, National Crime Agency.

5 *U.S. Efforts to Combat Trade-Based Money Laundering*, U.S. Government Accountability Office, December 2019.

believes that there are specialist "International Controller Networks" that launder money for criminals through various methods, including TBML[6].

However, TBML is difficult to identify because it is integrated into the economy through trade transactions. It is therefore important for companies to include TBML as a type of risk to in their compliance risk assessments and, in the course of business, to be alert to "red flags" that may point to potential TBML. The NCA has provided the following informational graphic setting out example "red flags" of TBML:



SOME RESOURCES

National Strategic Assessment of Serious Organised Crime 2020, National Crime Agency:

https://www.nationalcrimeagency.gov.uk/who-we-are/publications/437-national-strategic-assessment-of-serious-and-organised-crime-2020/file

National Crime Agency guidance on Suspicious Activity Reports (SARs):

https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-illicit-finance/suspicious-activity-reports

Trade Based Money Laundering, Financial Action Task Force, 2006:

https://www.fatf-gafi.org/media/fatf/documents/reports/Trade%20Based%20Money%20Laundering.pdf

At Your Service, Transparency International UK, 2019:

6 *National Strategic Assessment of Serious Organised Crime 2020*, National Crime Agency.

file:///C:/Users/PW053610/Desktop/Reading%20material/Money%20Laundering/TIUK_AtYourService_WEB.pdf