AASG
Accountancy AML Supervisors' Group

Open Account Trade Based Money Laundering (TBML)

Extracts from NCA Amber ALERTS of: June 2015 to March 2018 **(**References: A0152–ECC; A0171-ECC; A0172-ECC; 0328-ECC; 0392-ECC; 0514-ECC)

Overview

You should review this alert if you are an accountant providing services to clients who utilise open account trade. It is intended to help you understand what it is and the financial crime risk it can pose.

Trade Based Money Laundering (TBML) is the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origins.

Traditionally, TBML has been associated with document-based trade transactions for which a bank handles process documentation to the underlying trade agreement (otherwise known as trade finance). Such a narrow focus ignores the abuse of open account trade transactions involving cash, cheques and wire transfers, which are used to a significantly greater degree than classic trade finance products.

World trade is commonly conducted on 'Open Account' terms. This is the widely accepted practice of sellers extending credit to purchasers and shipping goods in advance of, and independently to payment. This is recorded as a book debt or a receivable against an open account with the seller. Payments to serve these debts are recorded as debits against the account, rather than as payment for a specific shipment, and can originate from a party other than the goods recipient. It is this process that is being misused.

For criminals wishing to launder money, this open account system presents an opportunity to remove the link between the recipient of goods, and the source of funds by settling the invoice through third party involvement. By using illicit funds to settle a legitimate invoice, and being reimbursed separately from the purchaser, criminals can hide the flow of their illicit funds.

Though the scale of the problem is un-quantified, the potential misuse of international trade as one of the ways criminal organisations, sanctioned entities and terrorist financiers can move money to disguise its origins and integrate it into the legitimate economy is deemed high-risk.

The Risks

Trade transactions where there is no clear connection between the payer and recipient of goods presents a number of risks:

- Using money hidden offshore to pay for goods that are then supplied into a legitimate separate corporate entity allows criminal funds to be re-integrated and can legitimise criminally derived wealth.
- Supplying goods between entities for no commercial reason can transfer criminal value, and can abuse the reputation of a genuine corporation through their supply of goods to an unknown recipient.
- Not tracking the source of funds for genuine supplies means corporate entities can end up dealing with opaque or disguised off-shore entities with no ability to risk assess the ultimate entity paying funds into their accounts.

Red Flags in Open Account TBML

- The originators of the payments are UK Limited Companies, Limited Liability Partnerships (LLPs) or Scottish LLPs incorporated by nominees and offshore company services providers or entities incorporated in international business centres (IBCs). The nominees are located in offshore

jurisdictions (British Virgin Islands, Seychelles, Belize, Marshall Islands, Dominica, Panama, Mauritius and Cyprus) or a small group of recurring firms in the UK and Ireland with links to these offshore centres. The offshore nominees and company services providers are often linked to adverse media relating to international money laundering or financial crime investigations and are sometimes referred to as 'distributors'.

- The sending banks for these payments are based predominantly in Latvia, although some are based in Estonia or Lithuania.

- The sellers account (global corporate client's bank account) is a global corporation with headquarters in Europe, Canada and the USA. They are exporting manufactured, agricultural, pharmaceutical or dual use goods. They hold beneficiary bank accounts in the UK and EU countries and have no relevant adverse media.

- The actual importer of the goods (as opposed the shell companies settling the invoices) tend to be located in the Commonwealth of Independent States region (notably Russia, Ukraine, Belarus, Azerbaijan, Uzbekistan, Kazakhstan). Limited information and no clear link or correlation to either the seller or buyer nor information that associates the entity with the nature of the import.

- Company receiving the payments is involved in import/export of goods to third world countries.

- Exact rounded transfers received into companies who sell low value, high volume products (Clothes, pharmaceuticals).

- Transfers only pay part of invoice (Company explains it is part payment of 15,000 invoice, but transfer is only 8,000).

- Transfers received in from companies/individuals who have no obvious link to the industry sector (Medical company paying for second hand clothing).

- The crediting account has been recently set-up and is receiving suspicious cash and transfers, followed by a final payment to the company. May be set up as a small business account (cleaning etc).

- Account holder of the crediting account is shown as living at a house of multi occupancy with little or no apparent connection to that property.

- Unusual or contradictory payment referencing (i.e. Ref - Car) when the payment is to a clothing company.

- If questioned, neither the payer nor the purchaser/recipient offers a valid, reasonable justification for routing the payment in this manner, often citing a ' debt' or 'tax efficiency' without providing details.

Suspicious Activity Reporting [SARs]

If you know or suspect ML or TF activity you should make a SAR and include the alert reference **0513-ECC** within the text *in addition* to the ongoing use of the Glossary of Terms.

Guidance on reporting is available at: www.nationalcrimeagency.gov.uk

Case Studies

The following case studies provide examples of identified typologies that have been used to launder proceeds of crime using TBML.

1 – UK Textile Recycling Business

UK textile recycling businesses have been shown to be receiving large amount of criminally derived money into their business accounts. It is believed the payments are part of a trade based money laundering system being orchestrated by international controllers mainly based in West Africa.

It is assessed that a large number of UK textile recyclers are receiving suspicious cash credits, credits from mule accounts, and electronic transfers directly funded by fraudulent activity into their business accounts. These payments are being made in order to pay for recycled clothing being exported to overseas customers, based predominately in West Africa.

It is believed that the overseas customers struggle to pay for the invoices issued by the UK textile industry and often turn to the black market in order to facilitate payment. This black market appears to be run by international controllers based in West Africa, who are using illicit cash to pay for legitimately generated invoices.

They then reimburse the criminals generating this cash with funds from genuine customers who turn to the black market to settle their invoices.

These international controllers are individuals who arrange the collection of criminal street cash from a variety crime types, including the sale of drugs and fraud, and deliver it to a chosen destination in return for a commission. They then co-ordinate trade based money laundering as a means of integrating criminal cash still further, and to facilitate cross-border payments without needing to transfer funds between jurisdictions.

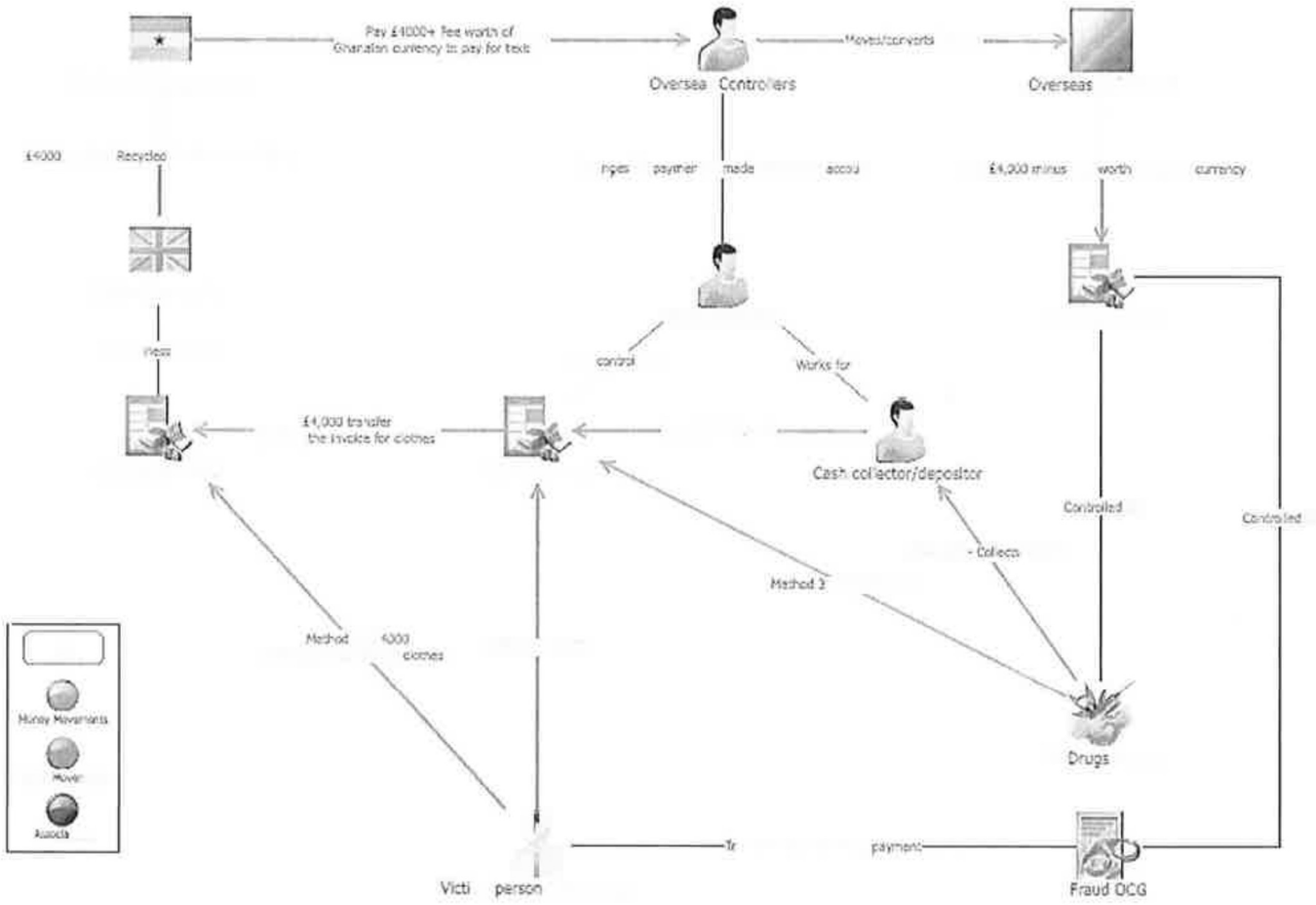
An initial assessment of the scale of the issue indicates that hundreds of millions GBP of criminal proceeds are being laundered with this methodology each year.

It is believed that the majority of criminal proceeds laundered in this way are generated through various types of fraud. There have been examples in which the victim of the fraud has been told to pay funds directly into the account of a textile recycler by the fraudster.

The system can also work with other crime types that generate illicit cash, such as drugs and organised immigration crime. In these circumstances, the controller in Ghana will arrange for members of his UK network to pick up cash from the crime group and then integrate it into the UK banking system using smurfing techniques and mule accounts. The payments are then made to the textile recycler.

The following is an example of the system in action:

- A Ghanaian clothing company in Accra has ordered 20,000 GBP worth of recycled clothing from a UK textile recycler and receives an invoice for payment.
- The Ghanaian clothing company approaches the controller in Accra and gives them 20,000 GBP worth of Ghanaian currency (plus a fee) with instructions to pay the business account of the UK textile recycler. It is believed that the Ghanaian companies use controllers because they offer better market rates and easier transactions; this is not necessarily an indication of complicity.
- In the UK, a fraudster has hacked a company's bank account and wants to launder 20,000 GBP from it. The fraudster contacts the controller in Accra and is told to pay 20,000 GBP to the UK textile recyclers business account with a reference of the Ghanaian clothing company in the payment instructions. (alternately this could be a drugs OCG depositing cash into an account to pay the invoice, or another source of illicit cash)
- The invoice has been paid and the clothes are sent from the UK to Ghana, usually via Sea freight transfer.
- In Ghana, the controller transfers 20,000 worth of Ghanaian currency, minus a fee, to an account under the control of the Fraudster.



2 – Abuse of Commercial Open Account System

The commercial open account system is the most commonly used method of conducting trade. It refers to the widely accepted practice of sellers extending credit to purchasers and shipping goods in advance of, and independently to payment. This is recorded as a book debt or a receivable against an open account with the seller. Payments to serve these debts are recorded as debits against the account, rather than as payment for a specific shipment, and can originate from a party other than the goods recipient. Much like the cash-in-advance system, where goods are shipped upon receipt of payment, only the invoice number is required to link a payment to a shipment. This open account system is used for the vast majority of global trading activity; the remaining trading activity takes place where there is a trade finance facility engaged relating to that trade, and is generally considered less at risk to this exploitation given the increased documentary scrutiny.

For criminals wishing to launder money, this open account system presents an opportunity to remove the link between the recipient of goods, and the source of funds settling the invoice through third party involvement. By using illicit funds to settle a legitimate invoice, and being reimbursed separately from the purchaser, criminals can hide the flow of their illicit funds.

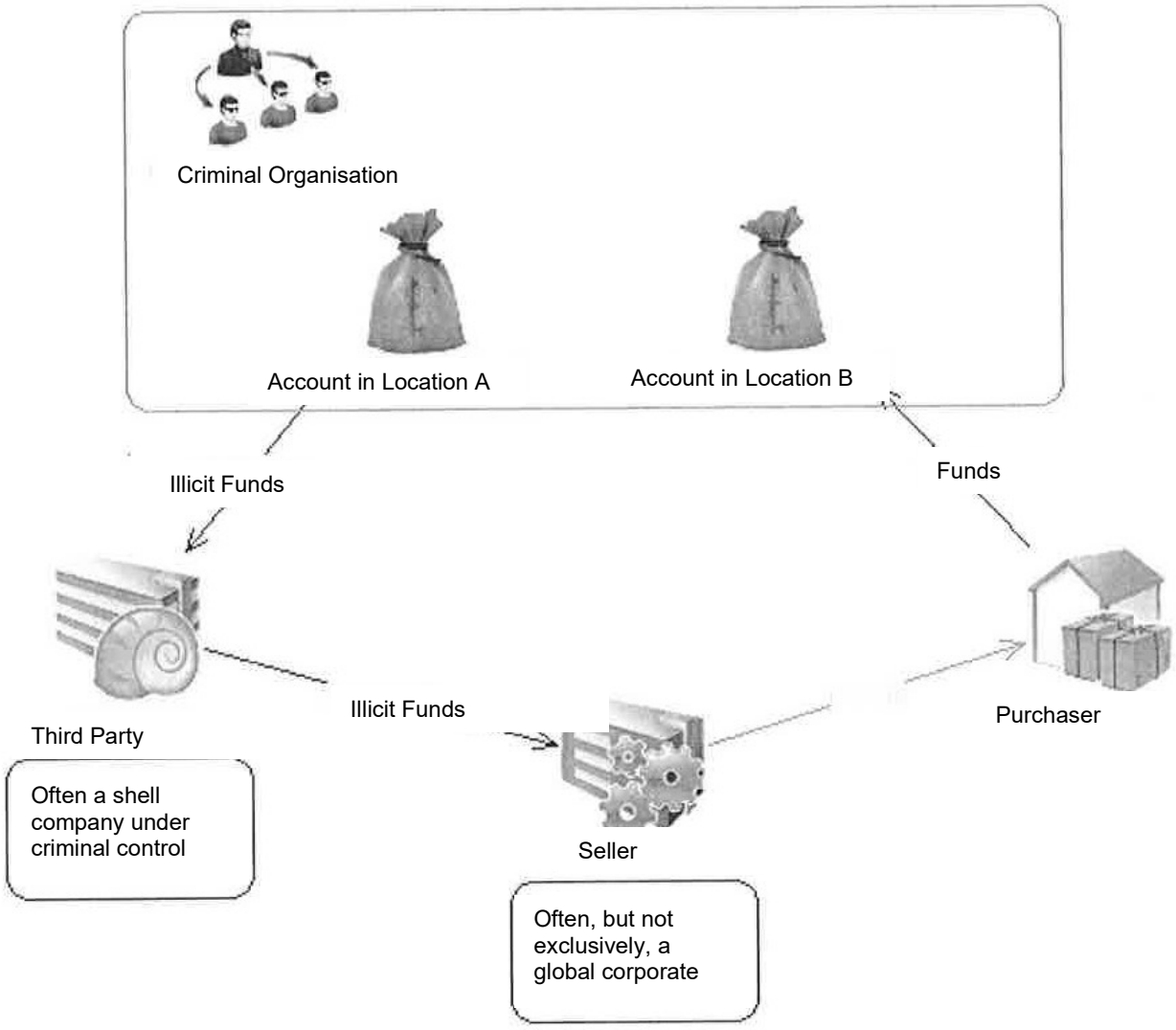
Third party payment methodology:

- A seller, often a global corporate but equally applicable to smaller enterprises, enters into a business agreement to provide products to a legitimate customer.
- An invoice number is produced relating to the particular order.
- Funds are received by the seller that correlates to an expected amount and invoice number, but from a third party unrelated to the purchaser.
- Goods are dispatched (or if goods were pre-shipped, the invoice is settled).
- The controller of the third party receives funds separately from the purchaser.

Unbeknown to the seller, the funds used to settle the invoice are of illicit origin.

- The criminals seeking to launder these funds have approached the legitimate purchaser of goods, and offered to provide a small discount on the purchase. Often they purport to be representing an import firm, or payment agent, who have agreed a deal with the manufacturer to receive a discount, and would hide their criminality from the true purchaser. This 'discount' convinces the true purchaser to use this purchase method, and is accepted by the criminal organisation as a cost of laundering the funds. The criminal organisation (purporting to be an import firm or payment agent) asks to be provided with the details of the invoice number, and funds for the transaction in an account in location B.

- They use illicit funds from a separate account in location A to pay for the goods



3 – Exportation of Goods to Former Soviet-Union states

Multiple bank accounts in the Baltic States controlled by UK registered companies funnel funds through a single UK account to make payments to corporates across the globe for goods to be exported to former Soviet-Union states.

Funds Are Derived From:

- 10 companies registered in the UK, Panama and the Seychelles with an unknown origin of funds.
- It has not been possible to determine corporate ownership, as the companies lack stated directors, correct Companies House filings, and public facing information.
- It is suspected that the companies directing payment are shell companies.

Funds Are Received Into:

- An Isle of Man registered company with a UK account whose director appears to be based in Ukraine.

Stated Business:

- The company stated that it was involved in the purchase of plumbing equipment from China and Turkey, for re-sale in Ukraine.

Movement of Funds:

- The company in question received approximately $5m USD, (£3.5m GBP) and sent approximately $4.3m (£3m GBP) in a 15 month period.
- Transactional analysis indicates that 98% (all but one credit) of funds were received from limited companies or limited liability partnerships (LLPs) banking in Latvia and Lithuania.

Destination of Funds:

- 84% of funds received by the Isle of Man company were then used to make payments to a range of import and export companies based in China, which is in line with stated business activity.
- Two UK registered companies received a total of $264,000 USD (£183,000 GBP) into Latvian bank accounts.
- The remaining recipients had accounts located in Turkey, the USA and the UAE.

Possible TBML Techniques:

- Corporate structure abuse. The opaque company structures of the UK companies may have been designed and created to obfuscate their beneficial owners.
- Secrecy of jurisdictions. The location of several companies in jurisdictions with minimal regulation regarding the recording of beneficial owners also obfuscates the controlling entities.
- Cash funnelling. The company central to this case study is acting as a cash funnel for 10 companies with unclear ownership and control, as well as acting as a conduit to pass these funds to various jurisdictions. This funnelling appears a further mechanism to obscure the origin of funds.
- Commingling of funds. Given that a large proportion of the company's activity is in line with its expected trade behaviour, it is assumed that some legitimate trade is taking place.

4 – Shell Company Banking in Latvia

A UK registered company owned by an offshore entity transfers funds to a UK registered shell company banking in Latvia.

Funds Are Derived From:

- Primarily (79%) from construction companies in Spain, Saudi Arabia and Turkey, which is line with the company's stated business.

Funds Are Received Into:

- A UK registered company, banking in Latvia, the ultimate shareholder of which is an entity registered in the British Virgin Islands.

Stated Business:

- The trade and export of timber and other building materials, as well as the raw materials for the ceramics industry.

Movement of Funds:

- The company was credited with $24.8m USD (£17m GBP) and transferred an equivalent amount in a 15 month period. This was ten times the anticipated business activity.
- Approximately 45% of funds were paid to shipping or building material companies, in line with stated business activity.
- Approximately 55% of funds were transferred to an account in Latvia, controlled by a UK registered LLP. This LLP is registered to an address associated to over 100 other companies, and its nominal owner is assessed to be a TCSP.

Possible TBML Techniques:

- TCSP/Corporate structure abuse. Regarding the recipient of funds, the use of a TCSP and an LLP to limit liability for the nominee director, obscures the controlling entity and allows a degree of removal.
- Secrecy jurisdictions. The company central to this case is owned by an entity registered in the British Virgin Islands.
- Commingling of funds. A large proportion of the trading activity matches the expected activity in this case. This suggests a commingling of illicit and licit funds, further disguising TBML activity.
- Ghost shipping/Over-invoicing. Whilst it is hard to identify given the lack of trade documentation visible, this may be a case of ghost shipping, or over- invoicing, as the payment details offer no verification of goods being shipped.

Data Protection Considerations

Please consider your obligations under the relevant data protection regulations and where necessary remove any related personal data from your systems securely and within a satisfactory timeframe.

Disclaimer