

Third party payments and trade debt settlements

Extract from NCA & JMLIT Amber ALERT - (Reference 0208-ML and 0210-ML 10.15)

Overview

Money laundering cases often involve an International Controller (IC) using a seemingly unrelated third party to settle a trade transaction. The aim is to transfer funds (the proceeds of crime) to a separate location. The recipient of the payment may not be aware of the true objective of the transaction.

As an amber alert it should be used to complement existing knowledge, to brief business teams and to support business process improvement (red alerts indicate more immediate or specific threats).

A case study is attached which you may find useful to provide further context to this alert.

How the transactions work

ICs have access to large sums of money in numerous locations throughout the world – 'cash pools'. Controllers can conceal criminal funds by receiving money into a cash pool in one location and paying an equivalent value, less charges, out on behalf of the criminal customer in another.

ICs 'hijack' a payment to a third party (the third party will be expecting a settlement from overseas) and use cash received from a criminal customer in the UK to complete the settlement. In this way, the IC is 'teaming and lading' the cash across unrelated parties, to conceal the criminal funds. The IC can continue the concealment by selling the original cash 'hijacked' to another IC.

The ICs' links to other criminal or black markets around the world (particularly China, Pakistan, India, Iran and South America) is a key factor for requiring cash transactions.

Typologies of the businesses involved

- A UK-based company is exporting goods
- Overseas customers who haven't directly paid for goods received – the customer will claim that there is an issue with obtaining GBP to pay. They might arrange for cash payments by small cash deposits at multiple banks throughout the UK.
- Exporting to countries where exchange control restrictions apply

Suspicious Activity Reporting [SARs]

If you know/suspect ML or terrorist financing activity in relation to this alert, you should make a SAR and include the reference XXJMLXX within the text in addition to the ongoing use of the Glossary of Terms. Guidance on reporting is available at: www.nationalcrimeagency.gov.uk

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

The Accountancy AML Supervisors' Group (AASG) accept no responsibility for any loss, damage or expense arising in connection with the use of information in this alert. Any use will be taken to signify agreement to these conditions.

Case Study – Third party payments

- A criminal customer in the UK contacts an International Controller and asks to 'purchase' £50,000 in euros in another EU state. The Controller and criminal customer agree an exchange rate that will generate a profit of 7% to the Controller (a typical sum). The Controller arranges for a 'cash collector', working for the Controller to collect the cash from the criminal customer.
- Once the cash has been collected, the Controller pays out the equivalent of £50,000, less his 7% profit, in euros to the criminal customer's contact in the other EU state, from cash the Controller holds in his 'cash pool' there. The cash collector retains the £50,000 cash and awaits instructions as to what to do with it from the Controller. This money now forms part of the Controllers' UK 'cash pool'.
- At the same time, a trading company in Asia wishes to purchase goods from a manufacturer in the Far East. The trading company does not wish to make the payment for the goods through its bank, possibly because the transaction has an illicit element to it (eg, the avoidance of exchange control regulations, evasion of import duty, under-valued goods). The trading company contacts a money service business (MSB) in the Asian country and asks them to make the payment on their behalf.
- The MSB agrees to carry out the transaction, and the trading company advances the money to complete the payment, and passes on the bank details of the manufacturing company in the Far East.
- Instead of making the payment directly, the MSB 'sells' the transaction to the International Controller, and sends him the bank details of the manufacturing company in the Far East. The MSB is now holding the money received from the Asian trading company and which forms part of the International Controller's 'cash pool' in the Asian country.
- The International Controller contacts the UK cash collector and instructs him to pay the £50,000 cash received from the UK criminal into the bank account of a UK based trading company (connected to the International Controller). The cash is paid in via multiple small cash deposits and banks across the UK.
- The UK trading company does not wish its bankers to question a large international payment apparently unconnected to their business and so engages a UK based foreign exchange company (FXC) to make the payment on their behalf. The FXC accepts the business, not knowing the origin of the funds and not understanding the purpose of the transaction. The FXC completes the payment to the Far East manufacturing company.