AASG
Accountancy AML Supervisors' Group

Money Laundering and Tax Fraud typologies involving unregistered MSBs

Extract from updated NCA Amber ALERT of March 2022 (Reference 0678-NECC)

Overview

This alert raises awareness of unregistered MSB operators providing payment services informally through personal and business accounts operated by banks and registered MSBs. Acting as an unregistered MSB in the UK is contrary to Regulations 56 and 86 of the Money Laundering Regulations and is a criminal offence. Case studies and red flag indicators are provided to assist in the detection Money Laundering and Tax Fraud. This alert is particularly relevant to accountants who may have MSBs as clients.

Money Service Business Overview

Money Service Businesses are described in law as businesses that act as a currency exchange office (bureaux de change), transmit money (or any representation of monetary value) by any means (money remittance), or cash cheques payable to a customer.

For the purposes of this Alert, MSBs include businesses that are natural or legal person(s) acting as non-bank financial institutions (NBFIs) such as payment service providers and electronic money institutions (with either e-money / payment services and/or money remittance permissions). This excludes persons dealing solely in cryptoassets but includes persons providing payment services using informal value transfer systems (IVTS).

There are currently approximately 31,000 registered MSBs operating in the UK, acting as either a Principal or an Agent of that Principal supervised under the Money Laundering Regulations (the MLRs).

A common benefit of using an MSB is that individuals and businesses use services without having to be a registered customer or hold an 'account'. MSBs are targeted by Organised Crime Groups (OCGs), because it is easier to access the financial system anonymously. More than 2.5 million UK consumers and businesses now use open banking-enabled products to manage their finances, access credit and make payments. Some consumers and businesses prefer to use an MSB to make cross-border digital payments because of more competitive exchange rates than were offered by banks.

The most common use of IVTS operated by high street retail operators is by consumers making migrant remittances who tend to make a cash payment and request a cash pay out to the beneficiary.

Typically, these businesses do not enjoy UK banking facilities. Commercial IVTS operators tend to enjoy UK banking facilities and can accept digital payments. OCGs tend to use both high street and commercial retail operators. It is lawful to act as a Hawaladar in the UK if the business is appropriately registered and complies with the MLRs.

This Alert focusses on the highest-risk MSBs which includes those providing payment services using IVTS settlement mechanisms. The most common form of IVTS is Hawala. The Financial Action Taskforce (FATF) report *'The role of Hawala and other similar service providers in ML/TF'* [1] describes reasons why Hawaladars are used. The list is not exhaustive but provides a useful insight into the drivers for the use of IVTS. The most common reasons cited were:

- Cheaper and faster money transmission
- Cultural preferences
- Lack of access to banking
- Higher confidence in Hawala than in the banking system
- Evade currency controls and international sanctions
- Tax evasion

[1] https://www.fatf-gafi.org/en/publications/Methodsandtrends/Role-hawalas-in-ml-tf.html

- Transfer or conceal criminal proceeds

Checking the registration status of a MSB

In the UK, most financial service activities must be authorised by the Financial Conduct Authority (FCA). The FCA maintains a register of authorised firms including those acting, or intending to act, as an MSB. The Financial Services Register[2] is a public record of firms, individuals and other bodies that are authorised.

It is important that if your firm acts for a Money Service Business that you confirm the client's registration to provide this service. You can make these checks using the Supervised Business Register.[3]

Red Flags

The following are potential indicators of unregistered MSB activity:

- **Low value tester payments** initially sent, often under 100 Euros after which, in the subsequent 24-48 hours, there is an increase up to hundreds of thousands of Euros being transferred. This may indicate cross-border payments linked to Modern Slavery Human Trafficking (MSHT) relating to adult entertainment/sex industry/sexual exploitation;
- **UK-based Trading/Shell companies acting as an intermediary**, receiving funds from the UAE before immediately transferring the funds to a third-party based in the European Economic Area (EEA) in Euros. Documentary evidence, typically involving trade with China which makes no commercial sense, may indicate money laundering, tax evasion, sanctions evasion, and/or unregistered criminal IVTS activity;
- **'Transfer of own funds'** may potentially be a way to mask the true nature of the transaction. Other terms included 'mandates' and 'settlements';
- **Widespread de-risking** in the MSB sector by banks has caused some MSBs to search for other ways of obtaining banking services. Typically, illegal MSBs use personal or business accounts (not linked to financial services, such as convenience stores and other high-street retailers, minicab / courier companies, companies providing education or visa services), to conduct unregistered money transmission. This may be manifested in more than one business being registered at the same address;
- **Use of Post Office branches** has increased due to bank branches remaining closed for much of the day during the pandemic. This also follows the intentional downsizing of retail bank networks, whereby an agreement has been reached for Post Office branches under 'Everyday Banking' to offer an alternative counter service to affected bank customers (Money Remittance);
- **The extensive use of Post Office counters** to deposit cash from Third Party sources. This has kept many transactions at arm's length as the Post Office is unable to exercise KYC controls upon cash deposits (Money Remittance);
- **Falsification of records by complicit and corrupt MSBs.** False or inconsistent addresses; inconsistent capitalisation and formatting; lack of genuine corporate logos; non-existent companies; inaccuracies in tax and payment calculations; no VAT or company reference numbers present (All MSB Types);
- **Clustering/Nesting** where multiple MSBs operate in close geographical proximity to each other. Evidenced by streets, postal code areas and even buildings where several MSBs are operating at the same time, offering similar services. Whilst there may be legitimate reasons for this, such as offering money transmission services to different customer bases/remittance corridors, this may also be an indication of or an attempt to mask criminal and unregistered MSB activity (Money remittance and Forex);
- **Unexpected Changes in account activity** - In some cases this might be a business account such as a care home, suddenly making money transfers that are consistent with money transmission. In other instances, it will be an individual, or groups of individuals, utilising personal accounts in the same way (Money Remittance);
- **Use and harvesting of mule accounts by OCGs**, for example as seen with Underground Banking and Charities Abuse. Accounts will lie dormant for a period of time (sometimes months) followed by high volumes of transactions being executed over a short period of time.
- **Transactions involving faith schools or certain charities.** Not-for-profit Organisations/Charities/faith schools in particular communities operating as unregistered MSBs, (primarily money remittance and cheque cashing) and offering Hawala banking and other informal financial arrangements.
- **Informal financial arrangements** include cheques being used as face-value/being honoured within the community by multiple-bearers as opposed to the named payee. The activity is prevalent in London Not-for-profit Organisations, Charities/faith schools.

[2] https://register.fca.org.uk/s/
[3] https://www.gov.uk/guidance/money-laundering-regulations-supervised-business-register

Case Studies

Case Study 1

An unannounced inspection of business premises of a convenience store, in South London was carried out in an HMRC Tax Enquiry. Evidence that the taxpayer was operating as an Unregistered Hawaladar (serving Ethiopia) was provided by the taxpayer's agent following the visit.

Adjusted Tax declarations following the visit (and previously undeclared) identified profits of £30,000 from acting as a Money Transfer business over three years. The subject was a former Western Union PSD agent. The subject stated that he was operating an EKUB loan scheme, and transfers funds to Somalia on a smartphone through his business bank accounts. He stated that he deleted messages on his phone once the transaction was completed.

15 bank accounts showed that he had transferred more than £4 million in 3 years. His accounts showed regular receipts of £35.72 for working tax credit. He regularly received low value credits, (many low hundreds of pounds, and typically under £3,000) from people throughout the UK.

Ethiopian names were often quoted in the payment message. For example, £500 transaction "Bill payment from Ethiopian name Ref: another Ethiopian name". Several payments stated, "Thank you from" followed by "Ethiopian name".

Case Study 2

An HMRC unannounced Tax Inspection identified an alleged unregistered Small Payment Institution based in Newry. An electrical engineers trading company (turnover exceeding £500,000) was charging an OCG £500+ VAT per week to transfer their criminal proceeds through his trading company bank account, (a payment service is not ordinarily vatable). Suspected Tax Evasion exceeded £100,000.

The trading company was onboarded by four Forex Traders based in Eire and London so that transfers could then be executed overseas on the instructions of the OCG which were given on e-mail. Transactions in the tens and hundreds of thousands of pounds were executed by the Northern Ireland company on behalf of the OCG totalling about £3.5 million.

The Company falsified invoices purporting to show trading in Chinese commodities to satisfy the FX Traders CDD requirements to justify the transfers of funds. The company also transacted through three high street retail MSBs. Invoices bearing the electrical engineers trading company name were found in Small high street retail MSBs that were serving African migrants in Plumstead South East London. The OCG were involved in Rag Trade fraud involving the export of charity donations clothing to Nigeria from Northern Ireland who fraudulently reclaimed £7 million VAT. The principal suspect was convicted of money laundering.

Suspicious Activity Reporting [SARs]

If you know or suspect that there has been money laundering or terrorist financing activity (including as a result of information provided to you by the NCA) and your business falls within the regulated sector, then you are reminded of the obligations to make reports to the NCA under Part 7 Proceeds of Crime Act 2002 and the Terrorism Act 2000. If you decide to make a report in this way you should adopt the usual mechanism for doing so, and it will help our analysis if you would include the reference **0678-NECC** within the text. This reference is specific to the Alerts process; where appropriate, we would ask that this is used in addition to the ongoing use of the Glossary of Terms. Guidance on making suspicious activity reports 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) accepts 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.