

AML alert: Illicit finance risks associated with NETPs acting as cross-border e-commerce traders

Extract from JMLIT Amber Alert Reference 0710-NECC. Published December 2022

Overview

In the UK, to act lawfully, online marketplaces (OMPs) involved in distance selling that are based overseas (i.e., NETPs) who make taxable supplies in the UK may have a liability to be registered in the UK for VAT even if they have no physical presence here.

The purpose of the paper is to raise awareness of the fact that some NETPs will be part of organised crime groups (OCGs) who are attacking HMRC's VAT system by fraudulently registering for VAT with the aim of submitting fraudulent VAT repayment claims and stealing revenue which reduces funds available for public services.

VAT repayment fraud by NETPs and OMPs

VAT repayment fraud by NETPs and OMPs is a threat to the UK economy. This fraud is often conducted in combination with wider organised criminal activity, such as money laundering through East Asian Underground Banking and criminal 'Daigou' who may act as UK-based cross-border e-commerce OMPs in networks that include overseas OMPs and others.

Additional information on East Asian Underground banking and criminal 'Daigou' published by the NCA in October 2019 can be found <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/445-chinese-underground-banking/file>.

Owing to digitalisation, this type of fraud is one that can be committed remotely and is therefore considered low risk for the NETPs and OCGs who seek to exploit the UK Tax systems. The lack of physical presence in the UK provides a level of security and perceived anonymity for those conducting the activity.

Case Study

HMRC identified 57 NETPs and OMPs (who were sole-traders and not registered companies) using common contact details that had registered for VAT at a single address. Although the traders are NETPs, the principal place of business (PPOB) registered with HMRC on the VAT registration document is a virtual office in the UK. The address is known to have been used as a PPOB by criminal Daigou companies.

The entities have submitted multiple variation requests to update the names of the business associated with the VAT registration number (VRN) and to register and remove bank account details.

Non-bank financial technology ("fintech") companies details were added to VAT registration details (instead of bank accounts) to receive VAT repayments. The format of a sort code and account number does not allow HMRC to differentiate between a bank account and a fintech 'virtual' account number being used on VAT registration forms.

The company submits a low-value tester VAT repayment claim (under £55) most of the first VAT repayment claims were £40 or under. Subsequent VAT Repayment claims are under £10,000 and typically, between £1,000 to £4,000. When HMRC contacted the business, most were non-responsive.

Potential Indicators of suspicious VAT repayment activity by NETPs and OMPs at UK hotspot addresses

The following are potential indicators of suspicious VAT repayment activity by NETPs and OMPs at UK hotspot addresses. These indicators should be considered cumulatively as grounds for further enquiry and escalation.

Address Indicators

- The use of Virtual/Flexible offices or mail forwarding businesses as communication address.
- A single address was used by all 57 companies.
- High volumes of businesses operating from a particular location than would be expected (for example, residential addresses with high volumes of VAT registered businesses).
- The address stated as the PPOB is residential address/Virtual office.
- PPOB/Correspondence address is the same as PPOB/Correspondence address used by criminal Daigou companies.

Business Indicators

- New business less than 2 years old.
- Sole-Proprietor
- Business activity relating to OMPs, cross-border e-commerce, online retail sales and distance selling.
- "Standard industrial classification of economic activities" codes commencing "46" or "47". For example, **47910** (Retail sale via mail order houses or via Internet).
- Sole proprietor of NETP is a foreign national.
- Regular changing of business name / sole proprietor name linked with VRN.

Financial activity Indicators

- Estimated turnover less than £10,000 per annum.
- Non-bank Fintech companies details were added to VAT registration details (instead of bank accounts) to receive VAT repayments.
- Low value (<£100) first payment debited to HMRC, followed by subsequent credits from HMRC.
- Payments credited from HMRC under £10,000.

Other Indicators

- Use of **QQ.com**, **126.com** and **163.com** email addresses.
- Unable to identify online platform by which business is conducted.
- Falsified or suspicious documents.
- Non-UK registered telephone numbers.

Suspicious Activity Reporting

If you identify activity which may be indicative of the activity detailed in this alert you should make a SAR and include the reference **0710-NECC and also HMRC Project Aldgate 22** in the text.

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) 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.