AASG
Accountancy AML Supervisors' Group

Baltic Displacement

Extract from updated NCA Amber ALERT of February 2022 (Reference 0682-NECC)

Overview

This is a summary of a JMLIT+ Amber Alert written by the Baltic Displacement Cell ("the Cell") of the JMLIT+ Money Laundering Public-Private Threat Group (ML PPTG).

This alert seeks to address the emerging risks caused by displacement of the open account Trade Based Money Laundering (TBML) typology, which in its most basic form involves incoming third-party payments from shell companies with bank accounts in higher-risk jurisdictions to settle invoices for goods. The typology is a persistent and prolific money laundering method that has underpinned high profile cases, such as the Russian laundromat, which was responsible for removing billions of illicit funds out of Russia and associated countries.

Information Report

The basic TBML typology involved exploitation of the international trade and open account payments systems to move illicit funds. Typically, an order for goods would be placed with a large corporate entity with a corresponding invoice being generated. Upon payment however, the incoming funds would be from a third party with an account in a higher-risk jurisdiction, rather than the buyer stated on the invoice. The third party was most often a shell company registered in a traditional tax haven such as the BVI and Panama, or the UK (including limited partnerships (LPs), limited liability partnerships (LLPs) and Scottish limited partnerships (SLPs)), and the accounts were held with Baltic banks (Latvia and Estonia being most common).

The risk of this basic typology remains high. Growing awareness of the open account TBML typology however, as well as the risks associated with shell companies and Baltic banks has led to increased scrutiny and subsequent controls. For example, in April 2018 the Latvian government banned banks from servicing shell companies. As a result, it appears that the typology may have evolved as criminals find new ways to circumvent these controls and continue to launder illicit funds out of Russia and associated countries.

Three possible displacement trends have been identified, as outlined below.

- **New jurisdictions of risk for incoming third party payments.** Movement of suspicious activity away from accounts at Baltic banks towards accounts at banks in Central Europe (Austria, Poland, Hungary, Czech Republic). These feature in both direct transactions, where suspicious shell companies are now seen to be holding accounts with banks in these jurisdictions, as well as transactions through correspondent banking networks, as below.

- **Correspondent banking (CBK) "nesting"**, whereby banks in higher-risk jurisdictions (predominantly the Baltics) now hold accounts with banks in lower-risk jurisdictions (commonly Central Europe), and are now making international payments via their correspondent bank. In this scenario the suspicious shell company still holds an account in the higher-risk jurisdiction, however CBK payments place more layers between the ultimate remitter and beneficiary of funds.

- **Rising involvement of Fintechs with Baltic bank accounts.** Increasing instances of payments from electronic money institutions (EMIs), payment service providers (PSPs) and other types of Fintechs with accounts at Baltic banks. Fintechs include those registered and regulated in the Baltic region, Central Europe, and the UK. These payments can be direct or via CBK channels, and similarly to above, the additional layer of the Fintech can create more opacity over the end-to-end transaction chain, particularly in instances where the payments are aggregated or the Fintech is stated as the remitter rather than the original source of the funds.

It is assessed that these displacement trends may be linked to the open account TBML typology and an effect of more stringent controls on known risk areas. However, this typology is one of many methods that

criminals are believed to be using to move illicit funds out of Russia and associated countries.

Case Studies

Below is a sample of case studies which form the basis of the emerging risks identified. These are mainly illustrating banking transactions but accountants may find the scenarios of interest.

1. A Scottish LP (SLP) suspected shell company registered at a TCSP address sent a rounded EUR 100,000 payment from an account at a Polish Bank to a global mobile marketing platform. The SLP's general partners listed on Companies House were signed by Hungarian nationals who had been associated with negative open source reporting related to suspected Russian financial crime. The SLP was also found to be operating in noncompliance with The Scottish Partnerships (Register of People with Significant Control) Regulations 2017.

2. A prominent Ukrainian PEP is suspected to have made a large number of high value purchases from a web of shell companies which he is believed to have ultimately controlled. The shell companies were mainly registered in the BVI and Cyprus and the purchases were for luxury goods including high-end furniture and expensive art work. The shell companies all held accounts with an Austrian bank, where the UBO was listed as a close associate of the PEP. The Austrian bank has featured in negative open source reporting.

3. An account review of a large corporate client following the detection of suspicious third party payments from shell companies with Latvian accounts (believed to be Russian Laundromat linked) also identified a number of suspicious third party payments from a Czech bank following the same patterns. Remitters of the funds included a Czech company with limited online presence (suspected shell company) and a Slovakian company, relatively young in age, with nominee directors in high risk AML jurisdictions, possible links to other entities making suspicious third party payments, and the same purpose of payments on swift messages as other suspect TBML activity originating from Latvian banks.

4. UK-registered companies with Czech bank accounts have been associated with suspicious payments linked to Ukrainian PEPs. Further investigation into the payments suggests a number of UK and overseas corporate structures are involved, including those registered in jurisdictions such as Belize, BVI, Hong Kong, Panama and Russia. The bank accounts are held in different jurisdictions, including Cyprus and Latvia, but mainly the Czech Republic.

5. A proactive review to assess incoming payments linked to possible TBML displacement into Austria identified a number of suspicious transactions through GBP CBK channels linked to one Austrian bank, wherein it was the direct remitter of funds but not the original source. The suspicious payments originated from Fintechs and EMIs with Estonian bank accounts, and on one occasion a Latvian bank account, where the Austrian bank was acting in a CBK capacity. The beneficiaries were also third parties detected through CBK channels (no direct clients). The majority of the Fintechs were UK registered and regulated by the FCA, however exposure to Lithuanian Fintechs, Bitcoin exchanges, crypto asset trading solutions providers and UK investment firms linked to Baltic banks were also identified. A number of common red flags were identified including large rounded amounts (e.g. GBP 60,000); payments to suspected shell companies (including UK LPs) with a lack of publically available information; payments to UK shell companies with accounts at Polish banks; links to known higher-risk TCSP addresses; links to Ukrainian and Russian UBOs; in some instances the purpose of payment was stated as 'loans repayment'; lack of visibility over parties in the end to end transaction change due to the CBK nature of the payments; negative open source reporting.

6. A research project was undertaken to identify possible displacement of illicit flows in and out of the former Soviet Union after increased scrutiny and controls were placed on Latvian banks. The project found that UK registered EMIs were being promoted on Russian language websites and that there appeared to be an internet trade in anonymous UK shell companies, with nominee directors and EMI accounts and licenses. The research also found that individuals and institutions formerly linked with Baltic banks fined for money laundering offences are now associated to UK registered EMIs, including

as directors and owners. Evidence was also found linking former directors of those fined Latvian banks to new Czech Fintechs.

7. A series of payments identified through CBK platforms whereby a UK FCA regulated Fintech, with an Estonian bank account, made a number of payments to a suspected Irish front company with a Polish bank account. The Fintech's Estonian bank held a CBK relationship with an Austrian bank, who processed international payments on its behalf. The Fintech was registered at a TCSP address however the address on the swift message was different. The beneficiary had no online profile to identify line of business and was linked to a Dublin address which Google Street view suggests is a residential address. 26 payments were made over a nine month period totalling GBP 276,387.40. No useful information stated on the purpose of payment and a lack of information was available to establish economic rationale and identify parties in transaction chain.

8. A proactive review was undertaken to identify jurisdictions with the greatest exposure to suspected Russian-linked illicit financial flows. Austria, Cyprus, Hungary and Czech Republic were identified as jurisdictions of risk for incoming payments. A deeper dive into the transaction related to the Czech Republic identified a number of suspicious transactions involving smaller Czech banks with significant non-resident client portfolios; EU incorporated shell companies; local Czech companies and non-resident companies having UBOs based in the CIS region; nesting, whereby Czech PSPs and Czech banks are providing services to overseas PSPs.

9. A proactive review was undertaken to identify jurisdictions with the greatest exposure to suspected Russian-linked illicit financial flows. Austria, Cyprus, Hungary and Czech Republic were identified as jurisdictions of risk for incoming payments. A deeper dive into the Hungary-linked payments identified four Hungarian entities with accounts at Hungarian banks, all seemingly with Ukrainian UBOs, engaging in significant USD activity in excess of their declared revenues (tens of millions rather than tens of thousands). The vast majority of activity was cross-border (less than 1% with Hungarian counterparties relating to tax, accounting and audit payments) and was undertaken with medium to large Ukrainian exporters, which investigations suggested were to facilitate trade with European commodities traders. Transactions between the four Hungarian entities were also identified, indicating a possible layering and obfuscation of source of funds. The activity also raised concerns that the entities may be acting as unlicensed MSBs for Ukrainian exporters.

10. In one case, 80% of the entity's identified debit transactions were wire payments to Asia (mainly China). Further investigation identified that the entity was trading outside of expected business activity – clothing, handbags and shoes as opposed to being a local truck, storage and food commodity company. Accompanying invoices lacked detail over the description of goods or value of payments, however identified that the goods were to be delivered directly to recipients in Ukraine. Open source negative news linked some of these Ukrainian recipients to multiple allegations of tax evasion in Ukraine, raising questions about the legitimacy of the invoices. Research into one of the other entities identified that the UBO is/was the owner/founder of multiple companies in Ukraine, some of which were also linked to negative news including multiple administrative, civil and criminal court cases in Ukraine.

Indicators

The following red flags, identified in the case studies above, are well known indicators of TBML and money laundering in general, and are not specific to TBML displacement:

- Third party payments
- Large rounded payments
- Transactions outside of expected activity
- Links to shell companies
- Located at high risk TCSP addresses
- Use of nominee directors

- UBOs based in high-risk jurisdictions
- Lack of visibility
- Involvement of PEPs
- Negative open source reporting on linked persons or entities

However, when combined with the red flags detailed below, it may be indicative of possible TBML displacement.

Jurisdictional Displacement

- (Third party) payments to or from banks in Central Europe (Austria, Poland, Hungary, Czech Republic) either directly where they have shell company clients, or indirectly through nested CBK relationships with banks in higher- risk jurisdictions (including Estonia and Latvia).
- Payments from banks in the Czech Republic with a significant non-resident client portfolio.
- Czech PSPs and Czech banks providing services to overseas PSPs.
- Hungarian registered entities (often commodities traders operating near the Ukrainian border) with Hungarian bank accounts engaged in significant cross- border activity and transferring funds to other Hungarian entities with a lack of economic rationale.
- Payments involving PSPs, Fintechs or EMIs with accounts at Latvian, Estonian or Czech Republic banks. Payments may often be through CBK channels.

Fintech Displacement

- Payments involving PSPs, Fintechs or EMIs with accounts at Latvian, Estonian or Czech Republic banks. Payments may often be through CBK channels.
- Payments involving UK registered EMIs that are promoted on Russian language websites, particularly where linked to the trade in UK shell companies with EMI accounts.
- Directors, managers or UBOs of UK, Baltic and Czech registered Fintechs and EMIs formerly linked to Baltic banks fined for money laundering offences.

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 glossary codes XXJMLXX, XXTBMLXX and the reference 0682-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