FINANCIAL CRIME

Keep Calm and Export!

Are financial institutions doing enough to stop international organised crime networks from infiltrating their customers' open account trade payment flows to launder the proceeds of crime?

Three years on since the shock referendum result, the UK has officially left the European Union. The UK has begun the process of negotiating a future trade agreement with the EU, as well as seeking to replace the 40 further international trade agreements the UK benefits from by being a member of the EU and which allow it to trade with 70 countries around the world (with which it currently conducts 60% of its total trade). Whatever your position was on Brexit, it is now time to try to make it work.

According to the UK's most recent trade numbers [1], only 10% of UK businesses export. Seven of our top ten UK export markets for goods and services are members of the EU, with the others being America, China and Switzerland.

As the UK 'goes it alone', the Government will encourage businesses to increase export activity with countries in Africa and the Middle East, and with key markets in Asia, including China and India. We have already seen this, with the UK's first ever UK-Africa Investment Summit [2], taking place in London on 20th January 2020, and with Presidents, Prime Ministers and senior members of governments from a number of African countries, hosting trade events in the UK in recent weeks, including Rwanda and Ghana. The opportunities presented by markets like Africa are too big to ignore.

Understanding the risks, as well as the opportunities

Large multi-national exporters have more experience trading into these higher risk markets. However, as many banks and other financial institutions get behind the efforts of the UK Government to encourage more small and medium-sized businesses to increase their exports to Africa, the Middle East and Asia, it is essential that both financial institutions and their exporter customers recognise and take steps to mitigate some of the associated commercial, legal and regulatory risks.

There are a range of risks of trading into higher risk jurisdictions, including compliance with local laws and regulations, understanding who you are doing business with and avoiding falling foul of international sanctions regimes and anti-bribery and corruption law. However, I will focus on

1 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836787/190924_UK_trade_in_numbers_full_web_version_final.pdf
2 https://www.gov.uk/government/news/pm-hosts-first-ever-uk-africa-investment-summit-in-london

how international organised crime networks (OCNs) target and infiltrate open account payment flows relating to the settlement of legitimate UK export trade, in order to launder ill-gotten gains and move value around the world.

The elephant in the room

Let's look at the numbers: the National Crime Agency (NCA) and international law enforcement have identified that the most significant volumes of money laundered globally is through the infiltration of cross border trade, by OCNs. It is extremely difficult to estimate the scale of money laundering in the UK. Many have tried (see RUSI Briefing Paper, The Scale of Money Laundering in the UK – Too Big to Measure? [3]) and estimates range from in excess of £90bn a year (Home Office [4]), £150Bn+ a year (Serious Fraud Office), through to billions of pounds a day (National Crime Agency). When you speak to law enforcement off the record, they will often acknowledge that even the highest of these estimates are probably conservative, and the actual numbers could be significantly higher (by multiples). As the Home Office admitted in April 2016 [5]:

"The UK remains the largest centre for cross-border banking, accounting for 17% of the total global value of international bank lending and 41% of global foreign exchange trading. The size of the UK's financial and professional services sector, our open economy, and the attractiveness of the London property market to overseas investors makes the UK unusually exposed to international money laundering risks. Substantial sums from crimes committed overseas are laundered through the UK. There is no definitive measure of the scale of money laundering, but the best available international estimate of amounts laundered globally would be equivalent to some 2.7% of global GDP or US$1.6 trillion in 2009 [6]."

To put UK foreign exchange trading (FX) volumes into perspective, daily FX volumes traded through London are in the region of $1.14 trillion. This threat does not just exist in the UK. In September 2019, members of the US Senate Financial Services and General Government Appropriates Committee described trade-based money laundering (TBML) as 'America's biggest national security threat that almost no one is paying attention to. It links together drug trafficking, human trafficking, terrorism, Hezbollah and dangerous counterfeit products'.

One of the main challenges, however, is that while the ways in which OCNs infiltrate trade payment flows are not really that complicated (as will be illustrated, below), the characteristics or 'red flags' can be difficult for financial institutions to spot, with traditional AML transaction monitoring. But the signs are there if you know what you are looking for and the consequences for both exporter and financial institution of being caught up in this money laundering activity can be serious.

What is open-account trading, and why is it targeted by international organised crime?

Approximately 80% of global trade is conducted on an open account basis. An open account transaction is a form of international trade payment, where goods are shipped and delivered before payment is received (or due). Typically, a UK-based seller (exporter) offers the overseas buyer (importer), payment terms of 30, 60 or 90 days. The overseas importer is often a wholesaler or re-seller, who is importing goods into their country in order to on-sell goods to local retailers, businesses or consumers.

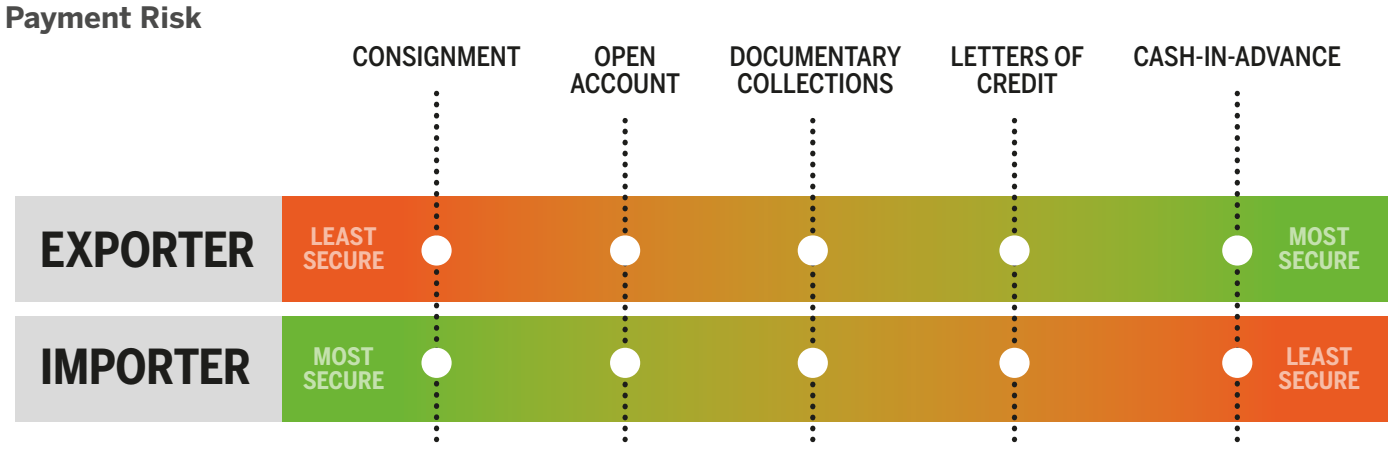

Diagram based on: Payment Risk Diagram, US Department of Commerce, International Trade Administration Website.

3 https://www.rusi.org/sites/default/files/20190211_moiseienko_and_keatinge_extent_of_money_laundering_web.pdf
4 https://homeofficemedia.blog.gov.uk/2017/12/11/economic-crime-factsheet/
5 https://www.transparency.org.uk/the-numbers-game-putting-a-figure-on-corrupt-flows-into-the-uk/
6 https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf

Open account payment terms are attractive to the importer, who takes possession of the goods before payment is made or becomes due. While open account payment terms are higher risk to exporters, exporters offer open account terms in order to be competitive and win and maintain business.

The other factor that is relevant here, and one of the reasons why international organised crime targets open account trade payment flows, is that with this form of trade payment, the remitting and beneficiary financial institutions involved in the transaction will not normally have sight of any documents relating to the sale and export of the goods, at the point the payment is initiated or at the point funds are received. As long as funds are received in to the exporter's account, and trade debt cleared in line with the agreed payment terms, goods will continue to be shipped, and the OCN can continue to launder their ill-gotten gains.

How does it work?

1. The UK-based exporter of goods receives a purchase order from one of its regular overseas importing clients, based in (for example) Africa, Asia or the Middle East (the Importer).
2. Goods are dispatched and shipped to an overseas port in the country of the overseas Importer.
3. In due course, the Importer wishes to make a payment to the UK-based exporter, in settlement of its trade debt, and so uses a local Money Service Business (MSB), FX broker or other Informal Value Transfer System (IVTS) to effect payment to the UK-based exporter. There are a number of reasons why a legitimate overseas Importer may prefer to use the services of an MSB, FX broker or IVTS, rather than making a bank-to-bank transfer, including to avoid higher FX/transfer charges, or local exchange controls, or because there are limited traditional banking facilities local to their place of business.
4. After receiving instructions from the Importer, the MSB, FX broker or IVTS contacts an 'affiliate' based in the UK, with instructions to make a payment to the UK-based exporter's UK bank account.
5. The UK-based exporter then receives a domestic payment, either cash, deposited straight in to its account, or an electronic transfer. It is informed that these funds are in settlement of the trade debt, relating to the sale of the goods shipped to its overseas Importer client. The UK-based exporter posts the payment to the client ledger.
6. The issue arises however, as the overseas MSB, FX broker or IVTS (or its UK-based 'affiliate') has connections to or is controlled by an OCN.
7. The funds that are received by the UK-based exporter in to its UK bank account are in fact the proceeds of crime, and are either:
   - Redirected proceeds of a fraud or scam* perpetrated on an individual or company by an organised crime gang, with the funds often routed through a series of bogus business accounts to make recovery harder, or
   - Cash of criminal origin deposited by money mules, frequently relating to the proceeds of narcotics, human trafficking, arms and sexual exploitation.

* The common fraudulent activity includes (but is not limited to): romance scams, investment fraud, account takeover, mandate fraud, invoice payment fraud and cyber fraud (including 'CEO impersonation' spear-phishing).

The OCN uses the UK-based exporter to 'launder' the proceeds of crime and move value between different actors within its international network. It extracts 'consideration' from a different point in the global enterprise, whether in the form of 'clean' funds, high value goods, or other criminal services.

The UK-based exporter and the financial institution with which it holds a bank account are used to launder the proceeds of crime, and are exposed to considerable commercial, legal and regulatory risks.

What are the risks?

For the exporter – 'I got paid, so why should I care?'

In virtually every case, there is a victim involved in this type of money laundering – a real business or individual who has suffered financial loss (or worse). Law enforcement may be involved, and this can lead to the initiation of criminal investigations. In some cases, there is an expectation on the exporter to return the funds that represent the proceeds of the fraud, or to account for the suspicious funds flowing through their business accounts. In other cases, the victim seeks legal redress against the exporter directly for the losses incurred. Where the exporter has already shipped the goods, they may be left out of pocket – and either has to request that their Importer client makes a second payment or has to make a provision in their accounts. Where the funds involved are significant, this can have a serious impact on the exporter's business.

Banks that are made aware of this activity may withdraw banking facilities from the exporter if they feel that the exporter has failed to address the issues properly, and has therefore exposed the bank to money laundering and associated regulatory, legal and reputational risks. This, in turn, has a significant impact on the continuity of the exporters' business, and its ability to trade, with the time needed to re-bank often being weeks, and sometimes months. In extreme cases, these issues have resulted in exporters going out of business.

For the financial institution

The primary risk for financial institutions is that their accounts have been used to launder the proceeds of crime. Where the activity has not been identified by their own transaction monitoring systems, the financial institution may face criticism and the regulator may initiate an investigation into the adequacy of the financial institutions' control environment, the actions taken by the financial institution and the extent to which they have complied with their legal and regulatory obligations. They may review historic activity and assess whether system-generated alerts have been properly investigated and suspicious activity reports (SARS) submitted to the NCA. Where law enforcement is involved, they may serve production orders or account freezing orders on the financial institution.

Where deficiencies are identified by the regulator, or where law enforcement investigations result in prosecutions and convictions, the financial institution may face censure and reputational damage.

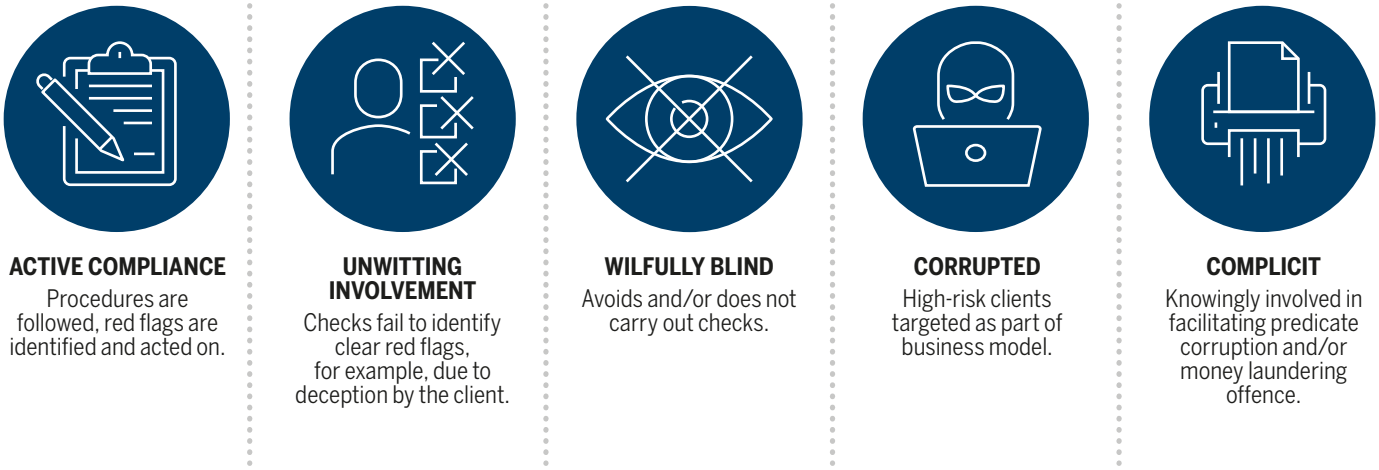

Diagram based on: Transparency International Report: 'At Your Service, Investigating How UK Businesses and Institutions Help Corrupt Individuals and Regimes Launder Their Money and Reputations' (Page 14, 'Nature of Involvement').

How widespread is it and can we quantify it?

These money laundering schemes can go on for years, undetected. The quantum of funds laundered through a single exporters' trading accounts can be significant (and material to its overall business). Sums range from one-off suspicious deposits of a few thousand pounds, up to tens of thousands, through to hundreds of thousands of pounds of suspicious deposits flowing into its trading account every week, recurring over many years.

Because of the difficulties in identifying this type of activity, it is not easy to accurately quantify the possible scale of money laundered by OCNs through open account payment flows of legitimate UK-based exporters. However, any UK-based exporter that sells and ships goods to higher risk jurisdictions and who accepts third party payments (payments that are not direct bank-to-bank payments from their overseas client's bank account), via unregulated MSBs, FX brokers and IVTSs, in settlement of trade debt, is exposed to the risk of this type of money laundering.

When set against the fact that 80% of global trade is conducted on an open account basis, it is the authors view that this activity represents a significant risk to businesses and financial institutions in the UK, and elsewhere. Inevitably, it is only a matter of time before there is a major high-profile exposé or scandal that brings to the public's attention how common this type of money-laundering is.

What are the steps exporters and financial institutions ought to take to mitigate the risks?

For financial institutions

- Where the financial institution has a branch-network, initiate staff training on identifying individuals who are seen repeatedly depositing large volumes of cash to different business accounts, reminding staff of their obligation to file internal SARS.
- Assess whether fraud and AML controls, processes and resources are appropriately aligned to the threat. For example, when a financial institution (financial institution 'A') is notified by another financial institution (financial institution 'B') that one of B's customers may have been victim of a fraud and that the victim's funds have been wrongly remitted to an account held at A, A should ensure the activity is reviewed for connections to the type of money laundering detailed in this article.
- Assess its total exporter customer population and conduct risk-based analysis of those trading with higher risk jurisdictions.
- Where appropriate refresh Business Activity Reports for export customers, to obtain up-to-date information on the country locations of key customers.
- Review fund flows to identify whether domestic payments (both cash and electronic payments) are in line with expected activity and Know Your Business (KYB).
- Sample closed AML alerts and internal SARs on the accounts of customers exporting to higher risk jurisdictions to assess whether further investigations are necessary (submit SARs to the NCA, as appropriate).
- Initiate education programs, targeted at exporter customers, focusing on the commercial and legal risks of accepting third party payments from unregulated MSBs, FX brokers and IVTSs, in settlement of trade debt.

For the exporter

- The exporter should advise their Importer clients that they will only accept payments directly from the Importer client (bank-to-bank) or via reputable registered and regulated MSBs or FX brokers.
- The exporter should screen payments for anomalous payment references or remitter details.
- Where possible, the exporter should not release goods until they are sure about the source of the payment. When goods are released to the Importer before the identification of an anomalous payment, the payment should not be posted to the client ledger.
- Where an anomalous payment is identified, the exporter should question their Importer client about the origin of the funds, and if the exporter is concerned about the source of funds, it should reject the payment and request a second payment directly from their Importer client (bank-to-bank) or via reputable registered and regulated MSB or FX broker.
- In consultation with legal advisers, the exporter may wish to consider amending its terms of business to enable it to reject payment, if the source of the payment is not clear.

For more information on how FTI Consulting can help you to combat financial crime, please contact:

Piers Rake
Managing Director
FTI Consulting
+44 (0)20 3727 1876
piers.rake@fticonsulting.com

FTI CONSULTING™

EXPERTS WITH IMPACT™

About FTI Consulting

FTI Consulting is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities.