



ARTICLE

Markets-based money laundering

Spotting the signs early

The Russian Laundromat case – in which several Russian individuals bought securities through Deutsche Bank’s Moscow office and concurrently sold the same through the bank’s London office – is one of few cases of money laundering involving the markets to make headlines in recent years. These ‘mirror trades’ transferred billions in roubles originating in Russia to dollars paid into offshore companies based in Cyprus and the British Virgin Islands between 2011 and 2015. The case resulted in the largest fine ever handed out by the FCA (£163 million) and revealed how large market players without adequate controls may be exploited to launder billions of pounds using relatively simple techniques.

And yet despite its high profile, the case has not resulted in sea-changes in the approaches taken by regulators and law enforcement to scrutinise how the markets can be abused to launder money, or in significant changes to how firms operating in this space control the risk of money laundering.

Capital markets are vulnerable to money laundering too

Capital markets are globally interconnected and predominantly highly liquid; vast sums moving between jurisdictions in fractions of a second present an attractive target for money launderers. And while retail banks have felt pressure in recent years to build more robust safeguards against money laundering, the same pressure has not been felt by wholesale market participants.

Instead, the significant regulatory developments made in this area have focused on managing the risks of market manipulation and insider dealing.

Market manipulation and insider dealing have as their main objective the generation of profit through trades that take unfair advantage of other market participants. In most cases, this causes a detrimental – and intentional – impact on the transparency and efficiency of the market.

Markets-based money laundering, likewise, involves the misuse of the markets for financial gain, and the trades involved may have an impact on market transparency and efficiency – thus meeting the general definition of ‘market abuse’. However, unlike market manipulation and insider trading, markets-based money laundering does not have as a direct goal the generation of profit – but rather, disguising the flow of funds.

“firm’s processes and monitoring tools are generally not designed to detect the typologies employed by this form of market abuse”.

This presents a challenge for regulators and firms alike. Except in cases where the source of the funds being laundered through the markets is also market manipulation, firm’s processes and monitoring tools are generally not designed to detect the typologies employed by this form of market abuse; for example, techniques such as identifying unusually high trading profits do not work where profit generation in itself is not the goal.

Complex typologies

The mirror trading featured in the Russian Laundromat is only one of a large number of typologies that criminals can use to covertly move funds via the markets – whether for laundering money, to circumvent sanctions rules, to fund terrorist activity, or to effect payment for illegal activity.

One example is equity placement, where a small-cap, publicly traded company with an offshore company as a majority shareholder issues convertible bonds to an individual. This sale is not disclosed publicly, and the bonds are then converted to shares worth significantly more than the value of debt purchased. These shares can then be sold to investors, allowing the individual to obtain clean funds into a UK bank account as a result.

Another example is compensation trading. Two market participants involved in a money laundering scheme carry out wash trades for the sole purpose of generating commission for a broker or brokers also involved in the scheme – resulting in the transfer of funds between the colluding participants and the broker.

Industry review

Regulators and evaluation bodies have published limited guidance to firms on strategies that may be employed to manage the risks of money laundering as it relates to the securities sector. This guidance is in most cases either outdated – such as the Moneyval and FATF reports published in 2008-2009 – or, as in the case of the 2018 FATF *Risk-Based Approach in the Securities Sector*, primarily focused on predicate offences that may lead into money laundering, including market manipulation and insider trading.

The FCA’s June 2019 thematic review *TR19/4 Understanding the Money Laundering Risks in the Capital Markets* is one example of recent guidance – that incidentally also exposes how lack of previous guidance may have impacted firms’ understanding of the risks in this area. In particular, the review found that “participants were generally at the early stages of their thinking in relation to money-laundering risk [in the capital markets sector] and need to do more to fully understand their exposure” and “many participants had not considered that potential market-abuse suspicions could also be indicative of money-laundering suspicions”.

“Between April 2017 and March 2018, the categories “Markets & Exchanges” and “Stockbrokers” accounted for, respectively, only 21 and 303 suspicious activity reports out of a total of 463,938 SARs made”.

The FCA’s assessment of the industry’s maturity should come as no surprise to those keeping an eye on the suspicious activity report (SAR) information regularly published by the National Crime Agency – the Financial Intelligence Unit of the UK. Between April 2017 and March 2018, the categories “Markets & Exchanges” and “Stockbrokers” accounted for, respectively, only 21 and 303 suspicious activity reports out of a total of 463,938 SARs made. This is a relatively low figure bearing in mind the multi-trillion-pound UK securities market. While several possible justifications for this figure exist, two betray more important underlying misconceptions.

- Firstly, market participants suspecting that money laundering may be occurring elsewhere in the market or trading chain believe that a submission of their own SAR is unnecessary. It is important to reinforce that all market participants have a legal obligation to report suspicious activity when they have a reasonable suspicion. Failure to submit a SAR may constitute a failure to discharge the obligation, resulting in a potential fine and reputational damage.
- Secondly, financial institutions may believe that market abuse related suspicious activity only requires a suspicious transaction and order report (STOR) to be submitted to the FCA. To dispel this misconception, the FCA published a letter giving guidance on the

distinction between both submissions. In short, STORs must be submitted to the FCA when there is a reasonable suspicion that transaction or orders could constitute insider dealing, market manipulation or an attempt to do either. SARs must be submitted when the firm knows or suspects an entity is engaged in money laundering or dealing in criminal property. Importantly, the legal obligation to submit a SAR is not satisfied when a STOR is submitted, and vice versa.

While market participants submitted only 324 SARs, they submitted 5,495 STORs over the same period. MiFID and Market Abuse Regulation provide a strong framework for reporting suspicious transactions, partly explaining the considerably higher number of STORs submitted. However, it is important that firms are encouraged to submit SARs as well as STORs. Where possible, authorities should attempt to simplify the submission procedure, avoiding duplicate reports and streamlining the process for often overburdened compliance functions.

The under submission of SARs is only one challenge facing Financial Intelligence Units (FIUs). Information sharing between authorities is becoming increasingly important as different competent authorities within a jurisdiction are responsible for different aspects of financial markets oversight. It is often the case that regulators will have a better overview of transactions within financial markets than FIUs. Similarly, resulting from the global nature of markets, competent authorities must ensure they communicate and collaborate with other jurisdictions when necessary.

Recent trends appear to suggest the information sharing between competent authorities is not only increasing in volume but also improving in quality, hence this might provide encouragement that competent authorities are better positioned to detect and prosecute money laundering within the securities sector.

Know your criminal

Firms currently place the burden of controlling the risk of markets-based money laundering on customer due diligence and risk assessment arrangements in the absence of trade monitoring designed to identify trades that may be being used to affect such a scheme.

For these arrangements to be effective, firms must identify and assess the risks posed by different products, customers, geographies and distribution channels. When they have assessed their exposure, firms may apply more resources towards mitigating the risks in areas of heightened vulnerability.

As an example, criminals attempting to launder their illicit proceeds will prefer large volumes and liquid markets, where large trades are unlikely to raise suspicions. As such, securities that can be used to convert currency, such as America Depositary Receipts, represent a greater money laundering risk than complex derivatives, such as thinly traded interest rate swaps.

Likewise, the size and complexity of security providers, as well as the number of intermediaries in each transaction will vary greatly. Hence, firms must consider whether they are dealing directly or indirectly with the ultimate clients, in the context of the services that they offer, and accordingly tailor their controls. Similarly, they must consider what risks are posed by their distribution channels and how they can be exploited by criminals to conceal complex ownership or to avoid monitoring thresholds.

“the high-risk, high-reward nature of markets-based money laundering means that these arrangements may simply be giving firms a false sense of security”.

Nevertheless, the high-risk, high-reward nature of markets-based money laundering means that these arrangements may simply be giving firms a false sense of security. The sophistication of schemes such as the Russian Laundromat – and the fact that in some cases the participants may be operating with state support – means that controls such as passport checks and risk assessment may be ineffective in determining the true identity of the actors involved. Activity-based controls, including trade monitoring, are needed to control the risk adequately.

Next steps

Despite the increased focus on market regulation in the last decade, the propensity for markets to be used for markets-based money laundering has increased due to the increase in the availability of higher risk products such as micro-cap investments, increased participation by retail investors and overall increased volumes of trades – as well as the introduction of better controls against money laundering in the retail space driving criminals to seek out new channels for the laundering of proceeds of crime.

To manage these risks, firms must study the typologies involved in markets-based money laundering and review previous cases – and revise their market monitoring tools to take these into consideration.

In the UK, the publication of the FCA's thematic review means that firms must consider themselves to be 'on notice' in relation to this issue and are under particular pressure to adopt more effective controls.

Abroad, firms should carefully monitor regulatory developments, and be prepared for similar thematic reviews and guidance in their home jurisdictions. Firms

struggling with the implementation of existing anti-market abuse controls – including those dealing with the technological challenges inherent in putting in place effective trade monitoring – must resolve these challenges now, before an inevitable 'second wave' of regulatory requirements is introduced.

The views expressed in this article are those of the author(s) and not necessarily the views of FTI Consulting, its management, its subsidiaries, its affiliates, or its other professionals.

FELIX JOHNSTON

Director

+44(0)20 3727 1772

felix.johnston@fticonsulting.com

FREDERICO BRANCO

Consultant

+44(0)20 3319 5626

frederico.branco@fticonsulting.com