August 2025 update:
This review is historical. See What we publish for more information and current views.

FINANCIAL CONDUCT AUTHORITY

Understanding the Money Laundering Risks in the Capital Markets

Thematic Review
TR19/4

June 2019

Contents

How to navigate this document

returns you to the contents list

takes you to helpful abbreviations

takes you to the previous page

takes you to the next page

prints document

email and share document

1 Summary

Introduction

1.1 The aim of this thematic review was to carry out a diagnostic piece of work looking at the money-laundering risks and vulnerabilities in the capital markets and, where possible, to develop case studies to help inform the industry.

1.2 In this report, by 'capital markets', we mean financial markets where shares, derivatives, bonds and other instruments are bought and sold. Our focus was assessing the risks, vulnerabilities and potential harm from money laundering in the secondary markets rather than the primary market. However, some of those we visited also offered primary-market services, and therefore we have included a section on this in our report.

What we did

1.3 We visited 19 participants covering different segments of the market. Our population included investment banks, recognised investment exchanges, trade bodies, a custodian bank, clearing and settlement houses, inter-dealer brokers and trading firms. When we refer to 'firms' in this report, we are referring to the full range of firms involved in the market transaction chain. When we refer to 'participants', we mean those firms we included in our sample for this project. Our visits were diagnostic; we sought information and examples to further inform and enhance our view of the risks and vulnerabilities in the capital markets. We did not assess the systems and controls of participants.

What we found

1.4 The money-laundering risks we have identified are mitigated to an extent by the nature of the firms in the market; most are regulated, institutional firms, and the nature of some of the products and markets may be less attractive to launderers, given barriers to entry, levels of scrutiny or complexity of the product.

1.5 However, there remain some risks particular to the capital markets, and we found that some participants need to be more aware of these. Our report highlights these risks. Furthermore, many participants told us they had used the FCA's Final Notice for Deutsche Bank in 2017 to build their understanding of money-laundering risks in their sector, but said they would find it helpful to have more examples of how money laundering might manifest itself to help inform transaction monitoring and training in particular.

1.6 As such, we have included an Annex to this report, which contains a non-exhaustive set of typologies built from a variety of intelligence sources. These typologies may help inform risk assessments, transaction monitoring and training. The Annex also includes questions that firms may want to consider.

1.7 We found that participants were generally at the early stages of their thinking in relation to money-laundering risk and need to do more to fully understand their exposure. It is apparent that our work has triggered further thinking in the industry, and in some cases has prompted firms to identify additional typologies or instances of potential money laundering.

1.8 We found that the nature of transactions in this sector means that effective customer risk assessment and customer due diligence (CDD) are key to reducing the opportunities for money laundering. Our report highlights that transactions often involve a large number of firms in a transaction chain, and therefore it is important that each part of the chain meets their obligations. The recent Upper Tribunal case involving Linear Investments Limited highlights the need for firms to have an effective surveillance system for transactions in place, rather than leaving it to others to monitor transactions.

1.9 Our work identified a range of approaches to anti-money laundering (AML) transaction monitoring and also highlighted some challenges and specific risks in relation to this. We found that participants' main focus was detecting market abuse, such as insider dealing or market manipulation. However, many participants had not considered that potential market-abuse suspicions could also be indicative of money-laundering suspicions.

1.10 We found that some participants were not clear on their obligations to submit Suspicious Activity Reports (SARs), and that focus in the capital markets had been on reporting market abuse.

1.11 We found that accountability and ownership of money-laundering risk in the first line of defence needs to increase, rather than be viewed as a compliance or back-office responsibility. In relation to training, some participants had developed a mixture of training delivery methods, and the training had been tailored to the risks faced by them. Others only used a basic online AML training module with little else to support it.

Potential money-laundering harm

1.12 Understanding the harm associated with money-laundering risks is key to our objective of protecting and enhancing the integrity of the UK financial system. In 2017, the UK National Risk Assessment of money laundering and terrorist financing assessed capital markets to be exposed to high risks of money laundering. This followed Deutsche Bank's Final Notice in 2017 for AML failings relating to 'mirror trading'. Separately, the Financial Action Task Force (FATF) published risk-based guidance for the securities sector in 2018. We recently published a Dear CEO letter for wholesale market broking firms which highlighted a lack of understanding and complacency about their responsibilities in relation to financial-crime risk, which includes money-laundering risk.

1.13 This report sets out our findings and further informs the view of the potential money-laundering risks and vulnerabilities in this sector. Below, we have set out a reminder of the legal and regulatory obligations of the range of firms in this sector, but that is only part of the picture. An effective regime needs more than applying a set of rules. As Mark Steward, Director of Enforcement and Market Oversight, said in his speech 'MiFID II and the fight against financial crime' on 3 July 2018 at the Duff and Phelps Global Enforcement Review 2018: 'Systems and controls will not work unless those systems inculcate the ability to ask the right question in a timely way, to be sceptical...and to stimulate both the ability and the desire to detect.'

1.14 Collaborative public-private partnership is also key to reducing this harm. We recognise that identifying and mitigating money-laundering risk in this sector is difficult. The global and complex nature of many of the transactions, combined with the multiple players often involved, exacerbates the challenge.

1.15 During this project, we have worked closely with others such as the National Crime Agency (NCA), which owns the SAR regime, and the Joint Money Laundering Intelligence Taskforce's (JMLIT) expert working group on money laundering through the markets. Many of those we visited were also members of trade bodies and industry forums that discuss and tackle money-laundering-related issues. These initiatives add real value, and we urge the industry to continue this work.

Legal and regulatory obligations

1.16 Firms authorised by the FCA under the Financial Services and Markets Act 2000 (FSMA) are required by our Handbook to have systems and controls to counter the risk that they are misused for the purposes of all types of financial crime, including money laundering, market manipulation and insider dealing. Recognised Investment Exchanges have their financial-crime obligations prescribed by section 2.10 of the Recognised Investment Exchanges section of our Handbook.

1.17 Separately, many firms (including firms not authorised by the FCA, such as lawyers and accountants) are also subject to requirements set out in the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the Regulations). The Regulations do not apply to all activities or firms within the financial sector, but they will typically apply to, among others, investment banks, recognised investment exchanges and providers of investment services under MiFID II.

1.18 Our Financial Crime Guide includes expectations that firms have robust systems and controls and governance arrangements. These should be based on a risk assessment of financial-crime risks faced by the firm, as required by the Regulations, that is comprehensive and considers a wide range of factors. The Guide also contains a chapter on insider dealing and market manipulation. Industry guidance produced by the Joint Money Laundering Steering Group (JMLSG) is also relevant, and the JMLSG is currently updating its chapter on brokerage services. Another useful source of non-binding guidance is the FATF's risk-based guidance for the securities sector.

1.19 Persons in the regulated sector are required under Part 7 of the Proceeds of Crime Act 2002 (POCA) and the Terrorism Act 2000 to submit a SAR if they know, or suspect, or have reasonable grounds for knowing or suspecting that a person is engaged in, or attempting, money laundering or terrorist financing.

1.20 The Market Abuse Regulation also imposes monitoring requirements on relevant firms to detect and report suspicious orders and transactions in the form of Suspicious Transaction and Order Reports (STORs). By 'market abuse', we refer to the civil offences that the Market Abuse Regulation has created, not the criminal offences of insider dealing or market manipulation. As such, a STOR is a means of submitting a suspicion of market abuse, and does not discharge a firm's obligation to report concerns of money laundering under POCA.

Next steps

1.21 We expect firms to consider their approaches to identifying and assessing the money-laundering risks they are exposed to in light of this report and Annex. We are also considering our supervisory approach in response to this work.

1.22 The recent enforcement actions against UBS and Goldman Sachs for MiFID I transaction reporting failures highlight the need for accurate transaction reporting by firms. Without accurate reports, the FCA's ability to undertake effective surveillance and monitoring is undermined. Mark Steward, Director of Enforcement and Market Oversight, said in his speech 'Partly contested cases, the pipeline and AML investigations' on 4 April 2019 at the Global Investigations Review Live event, that where firms use transaction reports within their surveillance processes, they should ensure that the data are correct and fit for purpose. We are also considering our strategy on how we can use MiFID II data to identify and mitigate money-laundering risk.

2 Our findings

Know your customer

2.1 We found that the primary driver of money-laundering risk is the customer, rather than products or delivery channels. We might have expected to find that some asset classes pose a high risk and others do not, but the typologies we include in the Annex show that money-laundering risk exists across various asset classes and scenarios.

2.2 We also found that the nature of transactions in secondary markets means it is likely that the order will be routed through multiple different firms, and a firm can generally only see their own direct customer; it is rare that one party can see the full chain.

2.3 These findings mean that effective customer risk assessment and CDD (including assessing the nature and purpose of the business relationship) are key, as firms depend on each other to perform these responsibilities well. For an effective defence against money laundering, it is essential that each firm performs effective CDD.

2.4 Participants told us that assessing the customer's intended trading strategies is key to understanding their business and an essential part of their CDD. Failings can have significant consequences, as illustrated by the Deutsche Bank mirror-trading case in 2017. Deutsche Bank failed to obtain sufficient information about its customers, which led to ineffective monitoring of trades. This meant that the mirror trades, which were highly suggestive of financial crime, continued undetected by Deutsche Bank for a considerable period.

Assessing the risk on a regular basis

2.5 Firms must identify and assess the financial-crime risks to which they are exposed, including money-laundering risk. The risk exposure might be a result of, for example, the products and services it offers, the jurisdictions it operates in or the complexity and volume of its transactions. Some participants included money-laundering risk in the capital markets in their business-wide risk assessment and had used red flags and risk indicators contained in public sources, such as the FATF guidance, to inform their business-wide risk assessment. Several participants performed a gap analysis against the Deutsche Bank Final Notice and considered what improvements could be made to their AML framework. However, some participants we visited had not assessed the risks posed by money laundering to their business at all. Some participants were solely focused on identifying market abuse and hadn't considered the risk that they may be used to facilitate money laundering. In these instances, participants struggled to articulate their view of money-laundering risks, and the discussion on this subject was limited.

2.6 CDD is important across the capital markets because understanding a customer's business model and trading strategies is key to subsequently understanding whether a customer's trading activity could be suspicious.

Lack of visibility of underlying customers and firms' interdependence

2.7 We found that most participants had no visibility of their customer's customer or, for example, the ultimate beneficial owner of the asset being traded. In the Regulations, there is no obligation to know your customer's customer. This means it is important that each firm in the chain is correctly fulfilling its obligations in relation to CDD for its own customer. While this is not unique to the capital markets sector, it is particularly important here, as trading chains often have multiple layers, involve complex products with many players and are often cross-border. A further feature of the Upper Tribunal case involving Linear Investments Limited is that a firm in the chain undertaking automated surveillance cannot eliminate the risk flowing from a failure by another firm to have its own surveillance system. Furthermore, firms must calibrate their automated systems according to the nature of their business and their customer's business.

2.8 For participants who use Direct Electronic Access (DEA) and delegate their system access to a sub-user, this creates a lack of visibility. We observed some mitigants for this risk, with some participants taking measures such as detailed questionnaires and on-site visits for DEA customers; gathering detailed information on risk-management controls; and achieving an in-depth understanding of the type of trading taking place.

2.9 Some participants we visited perceived that others in the transaction chain, such as the exchange or the custodian bank, were more responsible than them for preventing money laundering. We also found that some participants relied heavily on their customers being regulated financial institutions, with little consideration of other risk factors associated with the customer. Firms should take a variety of risk factors into account when considering money-laundering risk associated with individual business relationships. The Regulations allow firms, under certain circumstances, to apply simplified due diligence (SDD), where the extent, timing or type of CDD measures is adjusted if the firm determines that a relationship or transaction presents a low degree of money-laundering risk. Where SDD is applied, firms should take a risk-based approach rather than simply defaulting to SDD. Firms should also document the rationale for any decision to apply SDD.

2.10 It is important that CDD information is kept up to date to ensure that when the firm is seeking to identify suspicious activity, it has a current view of the customer's profile.

2.11 The Regulations say that firms must apply CDD measures to existing customers if the factors relevant to that customer's risk assessment have changed. Those factors include changes to the nature and intended purpose of the business relationship, or the identification of suspicious activity relating to that customer. This also includes those situations where SDD may currently be applied, such as when the customer is an authorised firm.

2.12 As part of conducting thorough CDD, firms should ensure they have appropriate oversight of who can instruct trades on behalf of a customer. Our review identified instances of potential suspicious activity involving orders from unconnected third parties. Effective CDD should help detect such instances and raise red flags.

Reliance

2.13 Firms are permitted to rely on a third party to carry out CDD. However, the relying party remains liable for any failure to apply such measures. If the CDD being relied upon did not meet the requirements of the Regulations, the relying firm would potentially be liable to civil or criminal enforcement action for CDD failings.

2.14 Reliance is not about relinquishing responsibility; rather, the relying firm retains responsibility but may benefit from efficiencies in both time and resources by avoiding duplication of CDD that another firm has already carried out.

2.15 As with our financial-crime thematic work in other sectors, most participants told us they were not relying on third parties for CDD, but preferred to do it themselves.

Enhanced due diligence and source of assets

2.16 Enhanced due diligence (EDD) is required in high-risk situations. Where participants had classified customers as high risk, for example high net worth individuals or customers with a connection to high-risk jurisdictions, we found some good examples of EDD. This included verifying the source of wealth and funds, as well as performing additional adverse media screening. We observed good practice where the complexity of an underlying corporate ownership structure was driving the level of EDD at the on-boarding stage, including assessing and challenging whether the complexity of the structure was commensurate to the rationale for the business relationship.

2.17 One participant mentioned that they had faced challenges in verifying wealth established over a long business history, explaining they would decline a business relationship unless sufficient comfort was achieved in line with their own customer acceptance criteria. Some participants had dedicated relationship managers providing enhanced ongoing monitoring of high-risk customers after on-boarding.

2.18 One vulnerability we have identified is the movement of assets (free of payment) between different accounts before being sold, eg if a UK firm allows a customer to transfer offshore securities into their UK trading account. These may be higher-risk situations, and therefore EDD may be appropriate. For example, one participant told us they obtained information about the origin of the assets being transferred to mitigate this risk.

Communication

2.19 Communication between firms is an important factor when considering how to reduce the potential harm from money laundering through capital markets, particularly where firms have concerns or suspicions. Generally, we found limited evidence of effective communication between participants who were a part of the same transaction chain, though one exchange did provide a good example of directly querying a member about unusual activities. This resulted in the latter identifying and reporting suspicious activity. We continue to encourage the industry to work together to share information where possible.

Transaction monitoring

2.20 Transactions in the capital markets are often complex, involving multiple jurisdictions and parties. We found that participants who used both automated and manual transaction monitoring were more able to identify suspicious activity than those using only automated systems. Most participants told us they recognised the importance of front-office awareness and escalations, which is where the majority of the typologies that participants gave us came from. We observed a potential disconnect between some participants' trade surveillance for market abuse and AML transaction monitoring functions, with the result that participants were not always recognising the potential for correlation between market abuse and money laundering.

2.21 Some participants were introducing initiatives to enhance transaction-monitoring capabilities, with increasing focus on network analysis and contextual monitoring, rather than monitoring driven by transactions alone. This reinforces the importance of good CDD, as due diligence information should inform the monitoring carried out on that customer.

2.22 Our Annex contains a list of potential red flags that may prompt questions when monitoring transactions for suspicious activity.

2.23 The involvement of different firms and jurisdictions in transactions often presents a challenge for transaction monitoring in the capital markets. While reliance can be useful for customer due diligence, the Regulations do not permit the use of reliance for transaction monitoring. Where a firm offers execution and clearing facilities for its customers and customers' underlying customers, the JMLSG (Part II, 18.23, 18.27 and 18.63) provides guidance on the need to adopt a risk-based approach to monitoring, emphasising the importance of understanding the business undertaken for its customer's underlying customer.

Transaction-monitoring findings

2.24 We found little evidence that participants had considered whether parallels may exist between their market-abuse surveillance and AML transaction monitoring. Some market-abuse practices (eg wash trading) may also be indicative of money laundering. The risk that money-laundering threats and vulnerabilities are not considered is increased where market-abuse surveillance teams and functions sit in isolation, or even in different jurisdictions, from their AML colleagues. Historically, the AML and trade surveillance functions in firms have largely operated independently of one another. But in many participants, we saw a growing synergy between the two, particularly in larger participants. We anticipate this more coordinated approach will continue.

2.25 Where large firms have multiple touchpoints with a customer, we observed that the existence of a lead relationship manager, or a key-person contact, provided a better level of oversight of the customers' overall transactions. This enabled the participant to understand the overall profile of each customer and to avoid a siloed approach to market abuse and other financial-crime monitoring. The context of understanding the customer and their business model was considered particularly helpful for the purposes of manual monitoring.

2.26 Effective automated transaction-monitoring systems are particularly important where there is no human involvement, ie where the trading is electronic, including DEA. We found that participants' automated transaction-monitoring approaches

varied in terms of the extent and depth of the money-laundering risks they were able to consider. Generally, larger participants had 'off-the-shelf' transaction-monitoring systems. Participants told us that their framework may include a combination of applying standard or pre-defined transaction-monitoring rules and thresholds, along with applying rules that are based on customer history and deviations from established patterns of behaviour. Where such systems have not been calibrated sufficiently for a firm's business model, there is a risk that monitoring may not be proportionate or appropriate to the specific risks faced by that firm.

2.27 Firms should be aware of the limitations of any automated systems for AML transaction monitoring. Where transactions are of a complex nature, involving multiple products and counterparties, an automated transaction-monitoring system alone may not provide enough coverage to mitigate risks. Several participants told us that the most valuable monitoring alerts or referrals come from manual monitoring or observation by the first line of defence rather than from systems.

2.28 We observed a risk where different entities within a group structure perform different parts of the AML transaction monitoring but may adopt different monitoring approaches. For example, firms that have an offshore custodian entity with an onshore execution broker entity may have different transaction-monitoring processes in place, with each acting in isolation.

2.29 Generally, we found that participants' AML transaction monitoring addressed the risk around excessive values of payments in and out of customer accounts. However, we observed that some participants were still developing transaction-monitoring rules to monitor 'free of payment' asset transfers or excessive asset transfers into custody accounts.

2.30 We found that some participants only monitored trading activity over a shorter time period, such as a rolling three-month period. This could create a risk that monitoring may not capture trading patterns with a lack of economic rationale, such as reversing positions, held over a longer period.

Role of platforms

2.31 Participants told us they perceived the money-laundering risk to be lower when transactions are conducted on exchange, as they thought exchanges may have better visibility of the overall transaction chain.

One exchange we visited had designed a front-end solution for access to its system. All traders need to come through an exchange member for access, but the solution meant the exchange could also see the location and other details of the traders, as users are required to provide this to obtain a login ID. The exchange recently added some software that identifies the IP address of those who log in. This information can be checked against where the trader says they are to identify users in high-risk jurisdictions, users who have given their location inaccurately or users who are mobile between several jurisdictions.

2.32 However, the other exchanges we visited could only see details of the member, and not the underlying trader.

2.33 We found it encouraging that some exchanges' monitoring activity had resulted in them raising questions directly with their members. This led to members reviewing their own customers. In one instance, it led to a member identifying customer activity that was assessed to be beyond that member's appetite for money-laundering risk, and the accounts were closed by the member firm.

2.34 As already noted in this report, each firm has its own role to play in the identification of suspicious activity, and while the trading platform might have visibility that other firms do not, equally, the bank or broker will have a different view and a better understanding of the customer's trading strategy and business model.

Non-standard settlement

2.35 We refer to settlement arrangements as being 'non-standard' in the context of a particular customer's usual trading and settlement. For example, if a customer informs their broker that the security should be delivered into an account held with a third-party broker, but this is not a usual instruction for that customer's account.

2.36 We observed a risk where one firm outsourced its settlement and custody arrangements, but where it had limited interaction with the third party to whom it had outsourced.

2.37 One participant told us that they refused to accept settlement instructions related to jurisdictions they had classified as posing high money-laundering risk. They also ensured that transaction monitoring could identify any involvement of these high-risk jurisdictions in the transaction chain. Settlement into high-risk jurisdictions is a risk factor that we observed some participants starting to include within their automated monitoring processes.

The risk of remote booking

2.38 Remote booking models make elements of transaction monitoring more difficult – for example, knowing the origins of orders and payments, as well as trades across different jurisdictions. We saw some participants with complex group structures executing transactions in foreign jurisdictions, which were then booked via an overseas branch into the UK.

2.39 Most participants recognised the risks around third-party involvement in payments, as these were risks observed in the Deutsche Bank mirror-trading case. Participants mitigated similar activity by being aware of the risks around third-party payments and third-party transfers of assets, and by implementing strong transaction-monitoring controls in relation to these.

Specific product/service risks for transaction monitoring

2.40 The use of omnibus accounts introduces challenges for transaction monitoring, as firms only see trades and payments at the aggregated level. We observed one participant providing omnibus accounts, but they did not appear to understand how many potential underlying accounts would be served. The JMLSG (Part II, 18.29) provides guidance where, using a risk-based approach, it may be appropriate for exchange-clearing members to on-board the underlying individual customers in an omnibus account, rather than only on-boarding the omnibus account customer. This will then allow for the application of appropriate risk-based transaction monitoring of those underlying omnibus account customers.

2.41 We found that participants had generally not prioritised efforts to enhance transaction-monitoring measures in relation to fixed-income products, and one participant we visited did not perform any automated transaction monitoring on fixed-income products. Despite this, it did not appear that any manual monitoring of fixed-income products was taking place, and the Head of Fixed Income could not give any examples where suspicious activity had been identified and escalated in relation to fixed income.

Voice and e-communications surveillance

2.42 Firms adopt electronic communications surveillance to address risks in relation to poor employee conduct and market abuse. Some participants told us that, given the potential correlation between some market-abuse behaviours and money-laundering behaviours, electronic communications surveillance is an existing resource that may also help to identify money-laundering risk. This is particularly true if electronic communications surveillance information is used to give further context to a transaction-monitoring alert.

We observed good practice where participants revised terminology or lexicons for their electronic communications surveillance systems to incorporate lessons learned from money-laundering case studies in the media, such as the Deutsche Bank case.

The future of transaction monitoring

2.43 We observed some participants exploring new AML transaction-monitoring approaches such as artificial intelligence, behavioural analysis and the adoption of a wider contextual and networking approach to automated monitoring.

2.44 Contextual or network monitoring is transaction monitoring in the context of a wider set of information about the customer or trade. The participants using network monitoring told us it can help them identify complicated networks or links between suspected parties or ultimate beneficial owners behind a transaction. Those participants using network analysis had seen a vast reduction in the number of false-positive alerts they received, when compared with using a traditional rules-based transaction-monitoring system.

Suspicious Activity Reporting

2.45 We found limited reporting by capital markets firms on suspicions of money laundering. Between April 2017 and March 2018, Markets & Exchanges and Stockbrokers (terms used in the NCA's SARs Annual Report 2018) accounted for only 21 and 303 SARs, respectively. This was out of a total of 463,938 SARs submitted to the NCA, predominantly by banks.

2.46 We consider the low level of markets-related SARs to be attributable to different factors, including firms:

- believing suspicious activity to be market abuse and, therefore, only reporting STORs to the FCA
- not having sufficient knowledge or capability to detect suspicions of money laundering through the capital markets
- having very few case studies and typologies, other than the Deutsche Bank 'mirror-trading' case
- thinking that money laundering may be occurring elsewhere in the market or trading chain, and therefore believing that a submission of their own SAR is unnecessary.

2.47 Our work included a review of capital-markets-related SARs. We found that internal reviews performed by some financial institutions, following the Deutsche Bank fine by the FCA, produced suspicious activity disclosures regarding the mirror-trading typology in particular. We observed that capital markets SARs are mostly submitted following a suspicion of market abuse, in relation to the proceeds of crime generated – for example, from suspected insider trading.

2.48 The NCA is exploring the introduction of a SAR glossary code for capital markets, which firms can use to 'tag' SARs relating to market activity. This would enable the money-laundering threat in this sector to be more easily identified and analysed via SARs and the JMLIT expert working group agrees that this would be useful. Our own reviews of SARs identified some features of trades that may indicate red flags for suspicious behaviour. These are included in the Annex to this report.

Understanding of reporting obligations

2.49 Some participants commented on the lack of specific industry guidance about when to submit a STOR, a SAR or both. They told us this generates uncertainty, as it is not always clear whether they must submit a SAR when a STOR has been made. The result was diverging approaches across the industry, with some disclosing a SAR every time a STOR is submitted. Others, however, believe defensive reporting provides little value to the already significant volume of SARs. Some participants said they would not disclose a SAR for attempted suspicious activity where no actual transaction occurs. The NCA's guidance states that as soon as you 'know' or 'suspect' that a person is engaged in money laundering or dealing in criminal property, you must submit a SAR.

2.50 The Law Commission published a consultation paper in July 2018 on changes to POCA, which also included a question on duplicate reporting. At the time of this report, the outcome of this review has not yet been published.

2.51 The quality of the SARs we reviewed varied. The NCA provides some guidance for when to submit a SAR and for effective drafting of SARs:

- Submitting a Suspicious Activity Report (SAR) within the Regulated Sector
- Guidance on submitting better-quality Suspicious Activity Reports (SARs)

2.52 Other guidance around suspicious activity reporting can be found in our Financial Crime Guide, as well as Part I, Chapter 6 of the JMLSG guidance. FATF's risk-based approach guidance for the securities sector provides a helpful list of red flags and risk indicators that may assist in identifying suspicious behaviour.

Reporting suspicions

2.53 We expect firms to have regard to their obligations under both the Proceeds of Crime Act, for submitting a SAR and the Market Abuse Regulation, for submitting a STOR. Reporting a STOR is a civil requirement and does not discharge a firm or an individual's legal obligation to report a SAR.

2.54 Some participants adopted a neutral approach upon receipt of an alert from the system as to whether the behaviour represented either market abuse or potential money laundering, or indeed another type of financial crime. This allowed them to consider their obligations to submit a SAR, a STOR, or both – independently of each other.

2.55 Some participants used a referral process where all STORs or suspicious activity alerts were sent to the money laundering reporting officer (MLRO) and financial-crime teams for consideration and, where necessary, further investigation. Some had introduced specific committees, composed of trade surveillance and AML staff, to consider alerts.

2.56 Some participants told us they had gathered further information on their customers' trading strategies from their customers when they were unsure if activity was suspicious or not. This helped them to decide whether to submit a SAR.

2.57 A few participants were unclear on whether they would consider suspicious behaviour as possible money laundering. One participant thought that their reporting obligations ended by submitting a STOR to the FCA. We reminded this participant of their SAR-reporting obligations under POCA.

Other barriers to reporting

2.58 There may be other barriers or circumstances that result in non-reporting of SARs; this includes not having sufficient details on the transaction. Where a decision is taken not to submit a SAR, it is important to clearly document and record the rationale for reaching this conclusion.

2.59 One participant described an over-the-counter bond transaction having no apparent economic rationale (the execution was outside the bid/offer price). Despite the customer twice attempting to execute the order via the trading desk, the transaction was rejected. The customer also wanted to involve a third-party overseas broker and was suspected of having prearranged a counterparty to the transaction. The participant didn't carry out the trade and subsequently submitted a STOR for attempted market manipulation. Despite some suspicion that the trade might have been attempted for financial-crime purposes (possibly related to tax evasion), no SAR was submitted even though the activities had raised concerns of possible money laundering. As the participant suspected money laundering, we would have expected them to have submitted a SAR in line with their obligations under POCA.

Behaviour and training

Behaviour and ownership of money-laundering risks

2.60 Our findings suggest that work is still needed to change behaviours within firms operating in the capital markets.

2.61 Poor behaviour across firms can undermine market integrity, creating harm and damaging confidence in the market. Our review established that the way in which firms identify and manage drivers of behaviour needs to change. This was particularly evident from interviews with staff in first-line sales and trading teams, where compliance and AML were sometimes seen as purely second-line functions. For example, first-line staff at one participant told us that they rely upon the Compliance and Financial Crime departments to assess money-laundering risks associated with their clients or trades.

2.62 There are parallels here with our findings on culture in the Deutsche Bank case. In that case, the first line failed to instil a sense of responsibility for the identification and management of non-financial risks. It also failed to appreciate that it was ultimately responsible for CDD.

2.63 At one participant, a desk head could not give any examples of money-laundering red flags and had to be reminded by the MLRO of the AML training they had received. We identified instances of conflict between first-line and compliance staff. One participant told us there was frustration because the on-boarding process was perceived to be longer than that of its competitors.

2.64 Conversely, we observed good practice where a participant encouraged accountability in the first line of defence by asking the business sponsor to attest that they were responsible for the customer, including that the business's CDD requirements for that customer would be met.

2.65 Participants who could evidence that they had considered the risk of poor behaviour were also more willing and able to contribute to a broader discussion on the risks and vulnerabilities in the wider capital markets.

2.66 We were told by several participants that staff in the first line have the best knowledge of clients and their trading activity, and as mentioned in the transaction-monitoring section, several participants commented that the most useful escalations originate from first-line teams. Ownership and understanding of money-laundering risk by the first line is therefore essential if firms are to have effective money-laundering controls.

2.67 Firms are reminded of their obligations under the Senior Managers and Certification Regime (SM&CR) which already applies to banks and the largest investment firms regulated by the FCA and Prudential Regulatory Authority (PRA), among others. The extension of the SM&CR will take effect for FCA solo-regulated firms on 9 December 2019. The extension of the regime will increase individual accountability for these firms, assess the suitability of senior management on a continual basis and hold individuals to account.

Training

2.68 Our thematic work found that money laundering in capital markets can be difficult to identify and detect. Most participants recognised that more knowledge and training are needed to help identify activity that could indicate money laundering.

2.69 We found that more training and subject-matter awareness are needed across the participants we visited. Firms should ensure that staff performing relevant roles receive tailored training on how money laundering could manifest itself. This should include any relevant typologies and red flags, such as those referenced in this report and the Annex.

2.70 We found that some participants only provide basic money-laundering training using e-learning modules. During discussion, some staff in these participants found it difficult to relate this to their business and the products they traded, particularly in the absence of practical examples. Others didn't appear to understand and appreciate the relevance of AML training. They viewed this as a necessary annual exercise to avoid a possible disciplinary process.

2.71 However, several participants had taken a multi-faceted approach to training and awareness. These combined e-learning with targeted face-to-face training delivered to relevant staff and resulted in better engagement with first-line teams. Participants referred to a healthy working relationship between the first-line and second-line teams, where staff raise suspicions or simply discuss instances of unusual activity with compliance or financial-crime teams.

2.72 Some participants use red flags, such as those contained in the FATF guidance, as part of their training. Firms should consider how the typologies and red-flag indicators in this report can be used to help inform risk assessments, transaction monitoring and training.

The primary market

2.73 Those participants we visited offered a range of services, so although our focus was on the secondary market, some visits involved discussions about the primary market.

2.74 The participants we spoke to perceived the risk of money laundering to be generally lower in the primary market. This was due to the extensive due diligence processes and layers of scrutiny by numerous regulated firms involved in, for example, premium listings and admission to trade on AIM. Participants also cited the involvement of lawyers in the primary market's due diligence processes as an additional layer of comfort.

2.75 One participant who acted as a nominated adviser (NOMAD) told us they found it harder to get comfortable with due diligence on AIM companies, as opposed to main market companies, as they tended to have more complex structures or hard-to-verify initial sources of funding. However, this risk is not unique to AIM companies. All firms acting as NOMADs to companies trading on AIM, corporate advisers to firms on NEX Exchange or sponsors for listings on the main market should note their obligations under the Regulations on CDD before transacting.

2.76 The perception of risk was higher in relation to some standard segment market listings where no sponsor or designated adviser is required at listing stage or on an ongoing basis. When there is no sponsor or designated adviser involved, but a firm (which may include a legal or accountancy firm) is nonetheless transacting with that issuer (such as providing advisory or underwriting services), it remains important that those firms understand and comply with their obligations under the Regulations to conduct CDD and EDD, if required.

2.77 However, while additional layers of scrutiny, particularly in relation to premium listings on the main market, may offer some additional comfort, those involved should not be complacent. The Securities and Futures Commission in Hong Kong recently fined several firms for failings in their role as a sponsor bank. Firms should also be aware of the risk factors when relying on the involvement of professionals such as lawyers, who can also be enablers of financial crime. The UK's National Risk Assessment in both 2015 and 2017 assessed there to be a high risk associated with abuse of legal services in money laundering. One example of suspicious activity a participant told us about showed how the involvement of a lawyer, practising despite being struck off, gave the illusion of legitimacy to a deal. The Office for Professional Body AML Supervision's report in March 2019 highlights the inconsistencies in the AML supervision of lawyers and accountants.

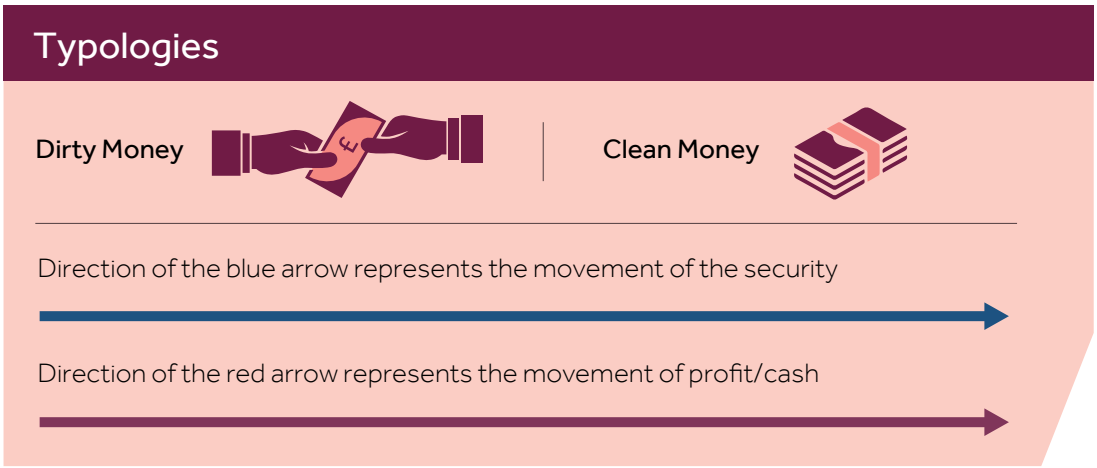
2.78 Scrutiny in the primary market takes place primarily through extensive due diligence. We observed that part of this process comes in the form of challenge through internal committees. Money-laundering risk in primary-market transactions can be mitigated by having a strong knowledge and understanding of the customer, and by understanding the business rationale for the transaction. We observed that some designated advisers or sponsors use extensive and often intrusive reviews by specialist investigators as part of their lengthy due diligence process for the listing of transactions.

Annex
Typologies

1. We had the opportunity to speak with many market practitioners about the risks they see across the capital markets. As a result, we have compiled some typologies that are not intended to be exhaustive. The aim of the typologies is to help inform. They are based on illustrative examples and they should be considered in the context of firms' or participants' specific activities and relationships. We hope that these will indicate to the industry where the vulnerabilities might lie in this sector and what the red flags might be, and that they will offer some questions to consider.

2. The examples below are built from a variety of intelligence sources, but they have been modified and developed with fictitious information to draw out the vulnerabilities. We are highlighting these as potential vulnerabilities, rather than saying that they are widespread crystallised issues in the UK capital markets.

3. We have included a number of diagrams to aid readers' understanding of the typologies. We have also added the following symbols to indicate where dirty money may be entering, and clean money leaving, the system, and to indicate the direction of travel of the security and profit.



4. Our work has identified some trade features that may act as a red flag to prompt questions or further investigation. We recognise that there are many good reasons that trades with the below features may take place, and the presence of these features alone does not necessarily indicate suspicion. This list is not exhaustive, and firms are responsible for determining the risks and factors relevant to their own business model. The features include:

- remote booking of trades between group entities
- pre-arranged trading
- instructions or involvement from third parties
- 'free of payment' asset transfers
- non-standard settlement arrangements
- uneconomic or irrational trading strategies of a customer
- unusual trading patterns, such as:

- counterparty concentration
- unusual win/loss rates or flat/neutralising activity
- no trading on an account

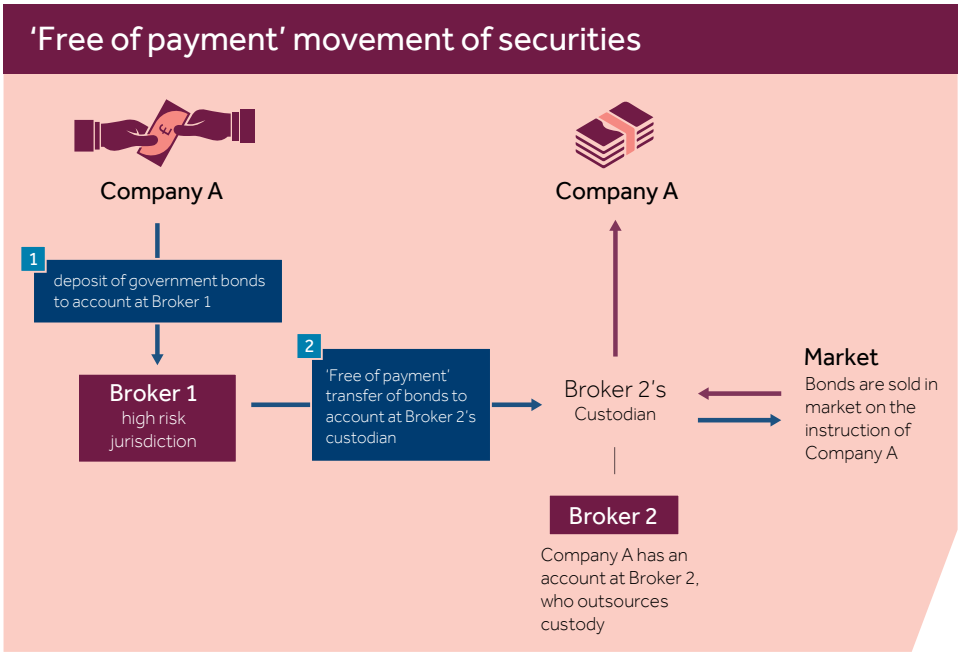
Example 1: 'free of payment' movement of securities

5. Company A is a customer of a UK broker's subsidiary ("Broker 1") in a high-risk jurisdiction ("Country 1").

1. Company A deposits a significant amount of offshore government bonds to Broker 1, who provides both execution and custody services.
2. While CDD checks are completed, including source-of-wealth checks, no checks take place to determine the ultimate beneficial owner of the bonds. The bonds are not registered in the name of Company A.
3. Company A then sets up a separate account with a different broker ("Broker 2"), in another jurisdiction ("Country 2").
4. Company A then requests that the government bonds are transferred into the newly formed account at Broker 2. Broker 2 accepts the government bonds into the customer's portfolio, without speaking to Broker 1 about their origin or ownership.
5. Broker 2 uses a third-party custodian, who takes delivery of the bonds. Broker 2 does not speak to their custodian to confirm ownership, including the source of the asset, or whose name the asset is in.
6. Company A then sells the government bonds.

Result

6. Company A has realised clean cash in Country 2.



Questions to consider

- What steps do firms take to confirm ownership of a financial instrument before it is deposited into a customer's account? How is this done for more opaque

instruments where there is no central register of ownership of the security? What documentation is provided by the customer?
- Are the checks conducted on an ongoing basis, ie when an account is already open and the customer then re-registers securities from somewhere else?
- How is the role split between the bank/broker and the appointed custodian/ administrator (whether part of the same financial group or not)?
- What is the firm's policy for accepting or rejecting securities that are not registered in the customer's name?
- What monitoring is done of accounts which only ever sell securities? Does this raise questions about where the customer is receiving their assets from?

Example 2: mirror trading

a. Mirror trading through a central platform

7. Two individuals sign up to two different brokerages in two different jurisdictions, one in a high-risk jurisdiction ("Country A") and the other in a different country ("Country B"). These two individuals are associates of each other.

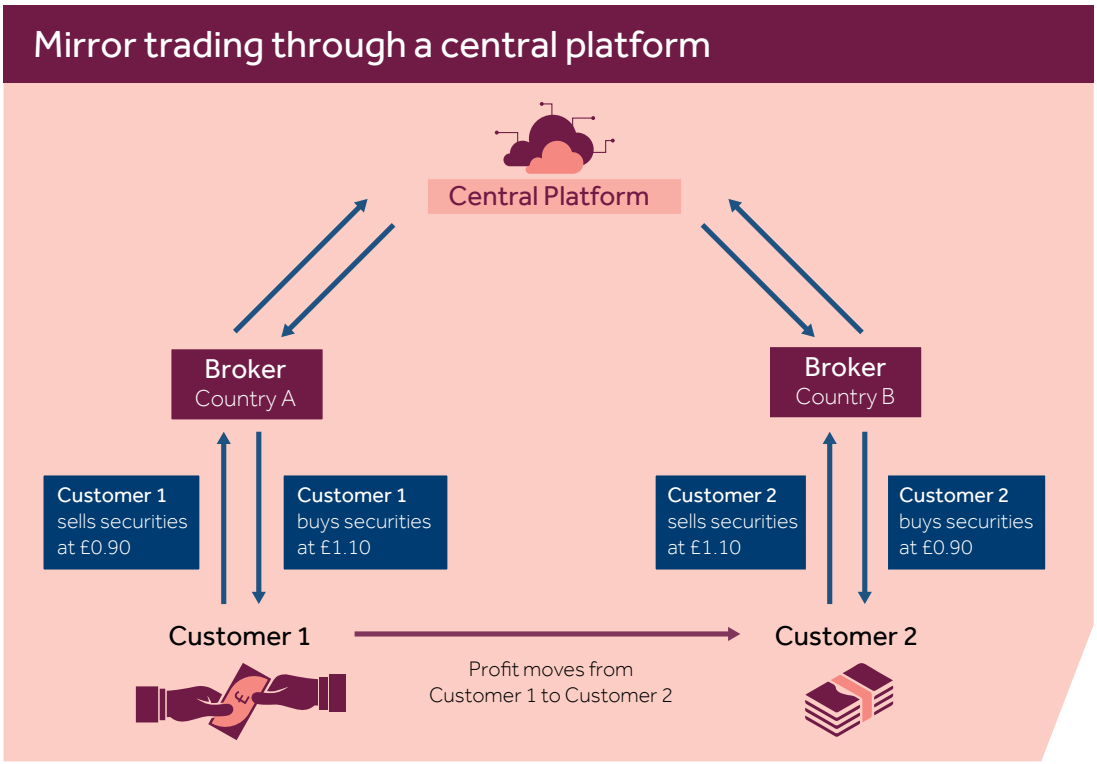
8. The two individuals tell their brokers they want to trade in particular options, and are provided with direct market access to a centralised platform with a lit order book to trade their intended contracts.

9. Once their access is established, the two customers choose to trade on the same market in the same security at illiquid times of the day, at which times they are the whole market.

1. The customer in Country B places orders to buy securities at a lower price (eg buy order at £0.90), and simultaneously places orders to sell the same securities at a higher price (e.g. sell order at £1.10).
2. The customer in Country A, being the only other participant, buys at £1.10 and sells the same securities at £0.90.

Result

10. The result is that both customers are flat in the security, ie neither had net bought or sold. However, money has moved from the customer in Country A to the customer in Country B.



Question to consider

- Do firms look for trading where the customer has an unusually high win or loss rate? If such activity is spotted, what steps are taken? Is the strategy questioned?
- What EDD and monitoring do firms do for customers located in high-risk jurisdictions?
- Can exchanges and platforms identify that two (or more) customers may be acting in concert, and only ever trade against each other? How do they do this?
- Is counterparty concentration a red flag in AML transaction monitoring?
- Do exchanges and platforms have the data to look for this typology?

b. Mirror trading off-market

11. Two customers (Customers "1" and "2") are associates of each other. They each apply for an account at two different brokerage firms in two different jurisdictions, Customer 1 offshore and Customer 2 in the UK. The number of each step below corresponds with the numbers on the diagram.

1. Once the accounts are set up, a third party contacts a third broker (Broker 3) requesting them to go to the brokers of Customers 1 and 2 (Brokers 1 & 2) and execute the following trades in steps 2-5. Broker 3 does not have sight of Customers 1 or 2.

2. Broker 3 buys securities from Broker 2 at £1.10 and sells the same securities to Broker 1 also at £1.10.

3. Broker 3 buys the same securities from Broker 1 at £0.90 and sells them to Broker 2 at £0.90.

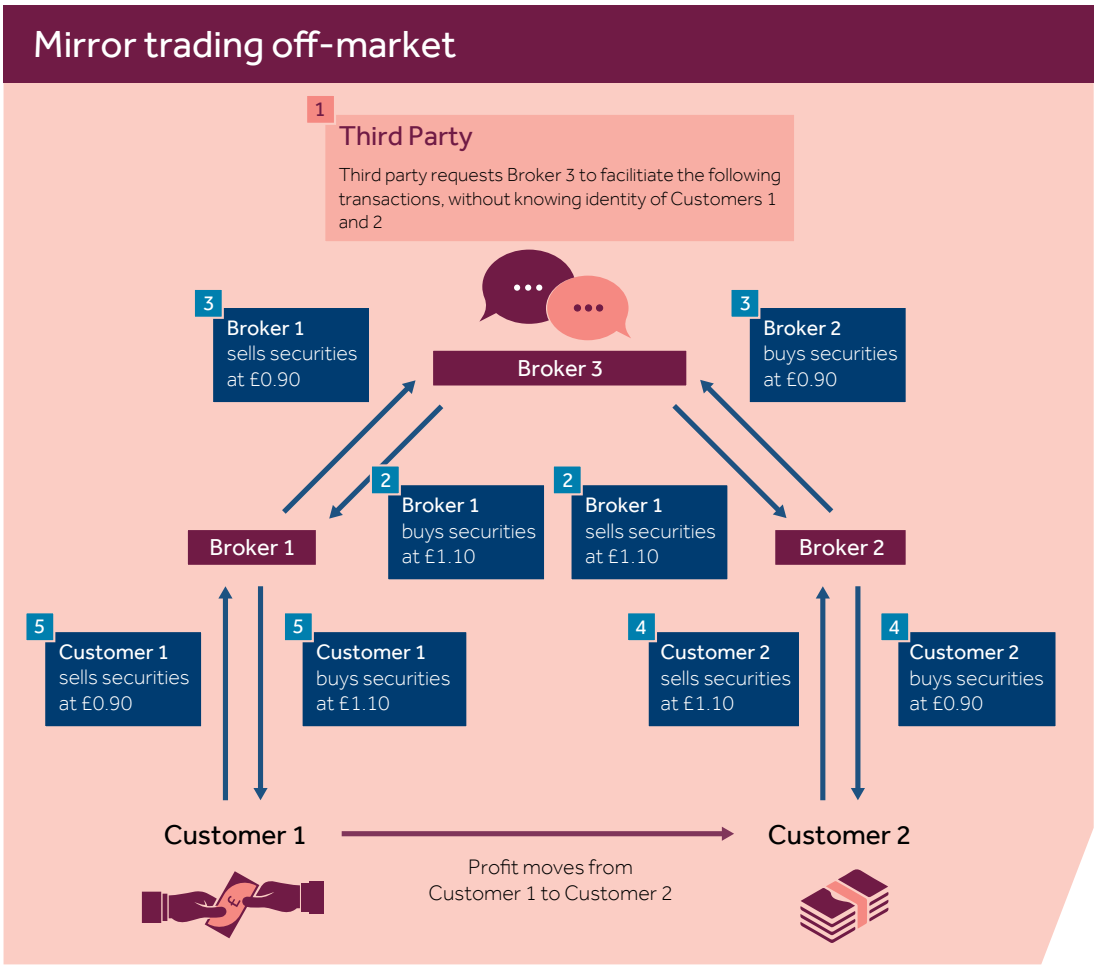
4. Broker 2 replicates the trades undertaken in steps 2 & 3 with Customer 2, ie Broker 2 buys the securities from Customer 2 at £1.10 and sells them back to Customer 2 at £0.90. This realises a £0.20 profit per share for Customer 2.

5. Broker 1 replicates the trades undertaken in steps 2 & 3 with Customer 1, ie Broker 1 buys the securities from Customer 2 at £0.90 and sells them back to Customer 1 at £1.10. This realises a £0.20 loss per share for Customer 1.

12. The market spread at this time is approximately £0.98-£1.02; this means that Customer 1 could get better prices by trading in the market rather than through the transactions above.

Result

13. Profit transfers from Customer 1 to Customer 2, though neither customer had a position in the security at the end of the transactions. The trading effectively acts as a mechanism for moving money from customer 1 to customer 2.



14. The FCA's Final Notice to Deutsche Bank in January 2017 is another example of mirror trading off-market.

Questions to consider

- What is the firm's policy on third parties instructing trades which are not for their account? What due diligence is the firm required to see before allowing such instructions?
- Does trading which is 'pre-arranged', (where the buy and sell counterparties are specified and already agreed) act as a red flag for AML?
- What would staff do if they identified such a scenario? Would they question or challenge the economic rationale of the strategy if their customer could trade more profitably on another market?
- What pre-trade and post-trade controls or surveillance do firms have in place for assessing the executed trade price against the market prices at that time?

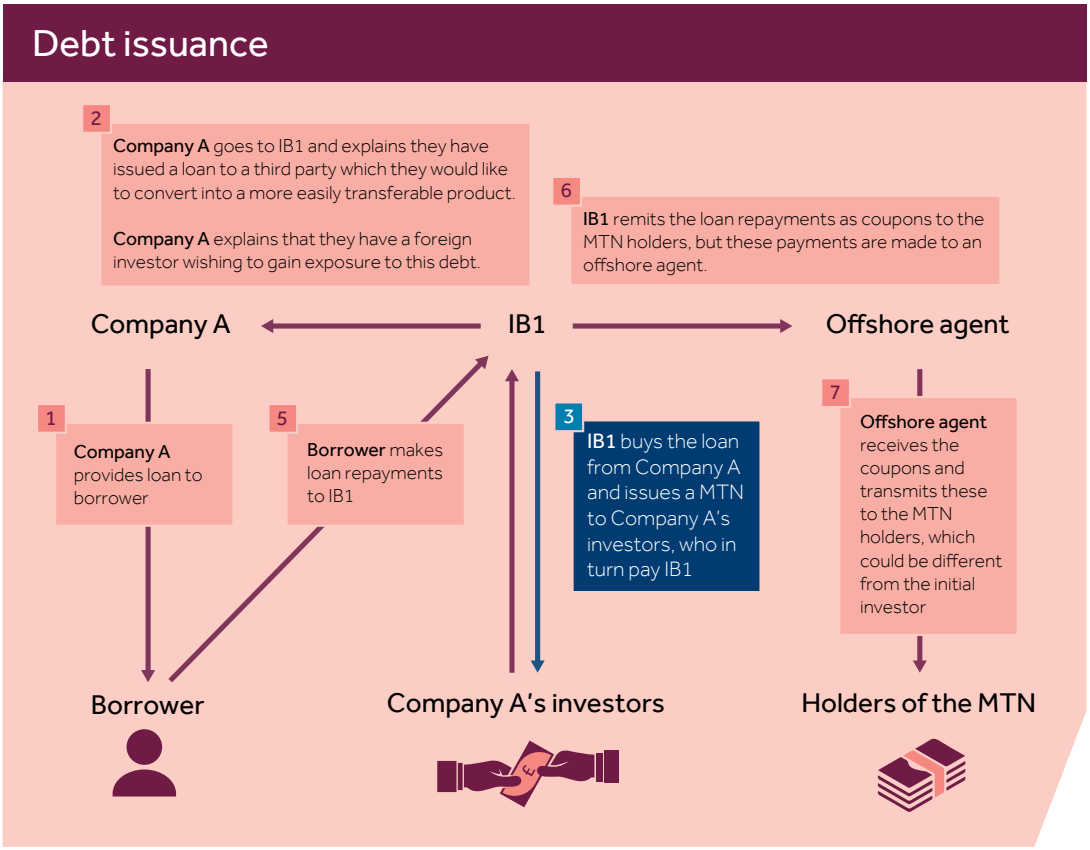
Example 3: debt issuance

15. The number of each step below corresponds with the numbers on the diagram.

1. Company A ("the arranger") goes to an investment bank ("IB1") and explains that they have issued a loan to a third party ("the borrower").
2. Company A explains to IB1 that they would like to convert the loan into a more easily transferable product, and that they have a foreign investor ("foreign investor") wishing to gain exposure to this debt.
3. Company A therefore asks IB1 to purchase the loan from them on a secondary basis and convert it into a medium-term note ("MTN") to be issued to the foreign investor (via Company A).
4. IB1 does not have sight of, or conduct due diligence on, the end investor but receives assurances from Company A that due diligence has been done.
5. Under the terms of the arrangement of the MTN, IB1 receives loan repayments from the borrower.
6. IB1 then remits these payments as coupons to the foreign investor as holder of the MTN.
7. However, the payments are not paid to the MTN holder/foreign investor directly, rather an offshore agent receives the funds and then transmits these on to the MTN holders, which could be different from the initial MTN investors.
8. It later becomes known that the underlying investor of the MTN is from a higher-risk jurisdiction and has significant links with the borrower ie the key controllers/shareholders of the foreign investor are the same as the controllers/shareholders of the borrower.

Result

16. The arrangement suggests a strong link between the borrower and underlying "lender" which could indicate potential embezzlement, money laundering or both.



Questions to consider

- When advising on the issuance of a security, do firms seek to understand any financial-crime risks involved with the product and their customers?
- Where a firm has been requested to issue notes/debt by an investor/representative of an investor, do staff consider whether there are financial-crime risks involved, in addition to credit risk?
- Do firms use agents to facilitate payments to underlying note/bond holders? What due diligence is done on such parties?
- Do firms assess the economic rationale for a complex transaction, including the presence or necessity for offshore agents receiving funds/assets? Do firms assess the risk arising from settlement instructions?

Example 4: equity placement

17. A small-cap company is admitted to trading. The company is majority-owned by an offshore company in a higher-risk jurisdiction, and has no assets to its name other than cash.

18. It issues a bond (debt), which can be converted to equity (shares in the company), receiving assistance from a UK advisory firm to do so. This is known as a convertible bond.

19. It issues the bond to an investor based in the UK. This individual has connections with a senior director of the company, though this was not disclosed publicly.

20. 30 days after the bond is issued, the investor decides to convert their debt into equity,

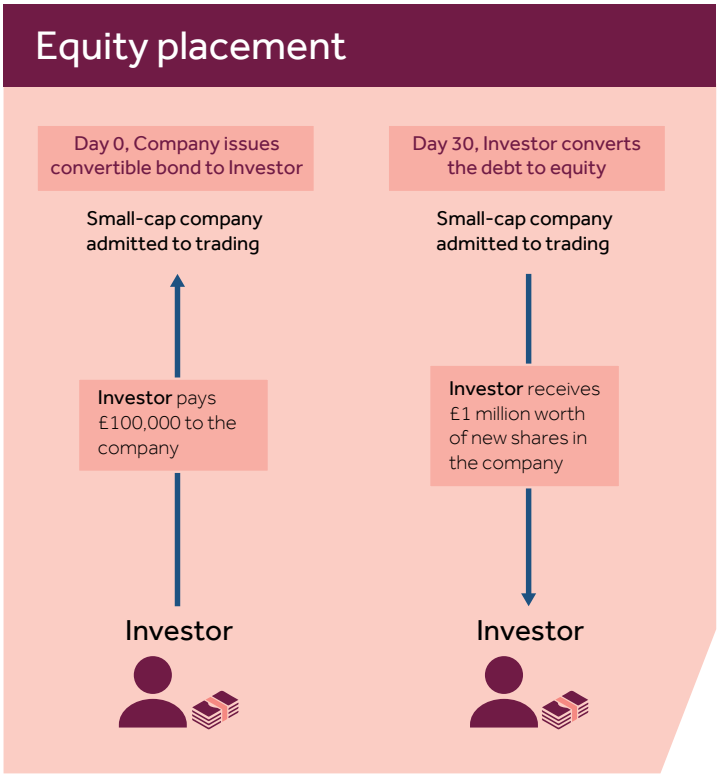
in accordance with the agreement. However, the notional value of the shares issued to the investor is significantly lower than the market value of the shares at the time of the conversion, ie the investor who lends £100,000 now receives the market value equivalent of £1 million shares in the company.

21. These shares are sold by the investor over the coming months, and the cash realised is then transferred into a UK bank account.

Result

22. It appears the activity was undertaken to wash illicit funds through the markets (and cross-jurisdiction) by lending money to the company, which was exchanged for shares that can be sold for more than the value of the loan. There are also other financial-crime concerns here, such as fraud.

23. While the issuance of debt offers some credibility to the transaction, debt is not required to be issued for the typology to be successful. The issuer simply needs to transfer new shares to connected parties, and then sell those shares in the market.



Questions to consider

- Do firms, when acting in an advisory/underwriting capacity to an issuer, consider (i) whether financing agreements are developed by customers on financially commercial terms, and (ii) the economic rationale of such arrangements?
- Do firms, when acting in an advisory/underwriting capacity, consider the risk of money laundering (and other financial crimes) by customers when advising on capital raisings?
- If a firm, when acting in an advisory/underwriting capacity, has identified questions/concerns that its customer may be unduly rewarding/compensating a particular investor(s) through an issuance of securities, what steps are taken? What questions are asked by the firm?

Example 5: intermediation

24. An offshore broker (based in a high-risk jurisdiction) regularly facilitates trading in government bonds on behalf of its customers.

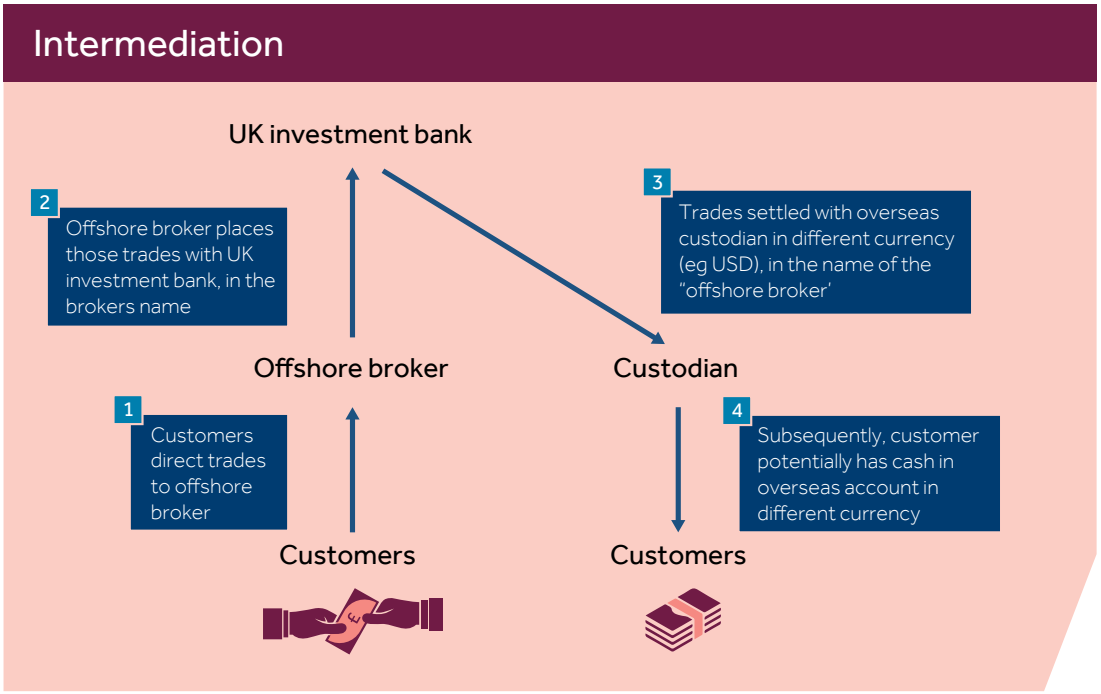
25. In order to access pools of liquidity for a particular bond, the broker uses the execution services of a UK-based investment bank. The UK-based bank does not treat the offshore broker as high-risk and therefore does not conduct EDD. The UK-based bank also relies on the offshore broker, as a regulated firm, to do CDD on its customers.

26. The UK-based bank allows the offshore broker to settle their transactions in a different jurisdiction in a different currency. This bank could simply see the offshore broker as its customer, ie an omnibus account; it could not see the broker's underlying customers.

27. It later became apparent, based on information the UK-based bank found in the public domain, that the underlying customers of the offshore broker were extremely high net worth individuals, some with political connections. It was also noted that the directors of the broker may have had close ties with some of those customers.

Result

28. As such, the bank has potentially been facilitating the transfer of economic value from one account to another, cross-jurisdiction, without realising that this might have been linked to financial crime.



Questions to consider

- Whilst recognising the potential limitations and difficulties for the UK bank in this scenario relying on a regulated entity to do full and proper due diligence, what questions would this raise about the level and quality of customer due diligence done by the broker?
- Does a firm ask questions to a broker at the time of taking them on as a customer such as:

  - What type of customers do you intend to onboard/have you already onboarded?
  - How do you assess whether a customer is high risk? What extra controls do you have in place in relation to high-risk customers?
  - How will you monitor for unusual activity by your customers?

- Do firms monitor for unusual trends in the trading done by their customers, which could be indicators of laundering? Have they considered what those trends might look like, such as only ever selling a security or an unusually high rate of losing/winning?
- Do firms monitor payments to/from institutions or geographical locations not fully consistent with the known geographic location of the client?
- Do firms consider on-boarding the underlying individual customers in an omnibus account, rather than only on-boarding the omnibus account customer, as per the JMLSG guidance?

Example 6: option premiums

29. A corporate customer (a broker in a high-risk jurisdiction) initiates a trade to open short-dated foreign exchange (FX) options positions. The trades result in the customer selling both an in-the-money call position and an out-of-the money put position in the same currency, at the same strike price and with the same expiry date.

Result

30. The effect of the activity is that the customer receives an initial premium payment into their prime brokerage account at a separate bank, only for this to be paid back upon the almost immediate expiry of the FX options.

31. The unusual trading is identified and highlighted via manual monitoring, as the bank cannot see a logical business justification for the pattern of transactions.

32. The neutralising effect of the trading raises concerns that the intended purpose is to facilitate the layering stage of a money-laundering scheme.

Questions to consider

- Before accepting the orders, would firms have asked the customer questions to understand the economic rationale of their trading strategy? How would the firms' systems flag the order where the order is electronic?
- Do firms monitor for uneconomic trading by their customers, which could be indicators of money laundering? Are option premium payments monitored as part of firms' AML transaction monitoring?

Example 7: account funding

a. Over-collateralisation

33. On a regular basis, a corporate customer provides too much collateral to its prime broker. The excess collateral is returned to the customer, but no questions are asked.

Result

34. It is suggested that the returned collateral may appear cleaner as a result.

Questions to consider

- Why is the firm's customer willing to regularly over-collateralise their account?
- Do firms identify this activity and discuss with their customer why it is happening?

b. No trading activity followed by cash withdrawal

35. A customer's trading account at a UK broker receives a significant amount of cash. The customer does not then trade on the account. Instead, two months later, it withdraws the cash to a third-party account.

Result

36. While the UK broker has no direct evidence of money laundering, it seems plausible that the cash was simply entered and withdrawn to make it appear cleaner.

Questions to consider

What controls do firms have in place around third-party payments? In what situations are they allowed?

- Do they look for unusually low trading activity on accounts? What do firms do in such situations? What monitoring controls do firms have on dormant accounts?
- Would a transaction involving funds of identical value, moving in and out of an account in a certain time period, be identified as a red flag?

Pub ref: 005892

12 Endeavour Square London E20 1JN
Telephone: +44 (0)20 7066 1000
Website: www.fca.org.uk