FINANCIAL CONDUCT AUTHORITY

Assessing and reducing the risk of Money Laundering Through the Markets (MLTM)

January 2025

Contents

Chapter 1

Summary

Background

1.1 Capital markets bring together buyers and sellers of stocks, bonds, currencies and other financial assets. They play a pivotal role in enabling economic growth and innovation by connecting entities seeking capital and investment.

1.2 Money laundering through markets (MLTM) is the use of these markets to launder criminally generated cash, so it appears legitimately generated. The UK's National Risk Assessment 2020 highlights that 'capital markets continue to offer a route for criminals to move and disguise the audit trail of money through the use of complex financial transactions'.

1.3 We carried out a thematic review (TR19/4) in 2019 and have continued money laundering supervision work across all relevant sectors since then. Based on significant further work and discussions with key stakeholders, we decided that it would be important to review progress and update our analysis.

1.4 Our report:

- Renews the risk assessment of MLTM and risks documented in TR19/4.
- Sets out the findings from our review. These will assist brokers and other firms operating in the capital markets to continue to improve their controls and ensure they meet the required standards. We provide insights and support through practical case studies and examples of good and poor practice.
- Facilitates further discussion across the markets to reduce the threat of MLTM.

Who this applies to

- Part 1 (Chapters 2-6) will be of interest to public bodies, firms and market participants responsible for assessing risk and setting strategy.
- Part 2 (Chapters 7-13) will be of interest to firms, MLROs and industry practitioners working in financial crime prevention roles.
- Part 3 (Chapter 14) will be of interest to firms and public bodies. This includes law enforcement, who are engaged in implementing strategic change to mitigate the risk of MLTM.
- By 'firms' in this report, we mean brokers and other firms operating in the capital markets.

What action should be taken

1.5 **A collaborative effort is required to reduce the risk of MLTM:**

- **Firms** need to continue to review their systems, controls, MLTM awareness and training to ensure they meet the required standards and are effective in the fight against financial crime. In particular:
  - Firms should consider and appropriately document the MLTM risk posed to and by the firm, ensuring it is reflected in their business-wide risk assessment (BWRA) and systems and controls.
  - Firms should consider how best to use transaction monitoring (TM) as part of an integrated process of financial crime systems and controls, incorporating tailored TM controls and alerts. Further collaboration between TM, TS, front and middle office teams should be encouraged and facilitated by firms.
  - Firms should ensure they have firm and role specific MLTM staff training and awareness in place.
  - Firms should ensure their relevant teams are aware of the UKFIU (UK Financial Intelligence Unit) MLTM SARs glossary code, are using it appropriately, and are submitting quality SAR reporting.
  - Firms should also review the recently enacted ECCTA (Economic Crime and Corporate Transparency Act 2023) and consider how they can share information to counter money laundering, raise awareness and intelligence and reduce MLTM risk.

- **Public bodies and firms** need to continue to work together to evolve and continue to improve the response to the threat of MLTM. In particular:
  - We will work closely with industry and partners to understand and share information on MLTM risks, issues, typologies and best practice.
  - We will ensure through our supervisory work, that firms are considering MLTM risks, and the points raised in this report to drive improvements and reduce risk across the markets.
  - We will work with firms and other stakeholders to establish if existing datasets can be better used to identify MLTM and enable further proactive supervision.
  - We will encourage greater innovation by firms and third-party providers so that TM systems and alerts become more tailored to capital markets.
  - We will work with the UKFIU to ensure better use of the MLTM SARs glossary code to raise awareness of suspicions.

Why we did this work and what we looked at

1.6 We reviewed the issues raised in TR19/4 and the progress made with combatting the risk of MLTM. We did this as part of our commitment within the Economic Crime Plan 2 2023-26 - action 17 and in response to financial crime concerns raised through our supervisory work and reported in Dear CEO letters (Chapter 5). We have also considered if there are any new or developing concerns since our previous thematic review.

1.7 We reviewed the financial crime systems and controls at a sample of wholesale brokers to understand how firms are approaching the following areas:

- business-wide and customer risk assessments (BWRA and CRA)
- know your customer (KYC) and customer due diligence (CDD) checks
- governance and oversight
- transaction monitoring (TM)
- investigations and suspicious activity reports (SARs)
- training

1.8 We focused our detailed firm reviews on wholesale broker firms (Chapter 5). Wholesale brokers play an important role in maintaining the effectiveness of UK wholesale markets. Their position in those markets, global trading, and the level of discretion they can have in bringing transactions together means they can have a significant impact on the integrity of markets. This also makes them vulnerable to exploitation for MLTM purposes. However, the findings in this report should be considered across wider markets and by other types of firms and business models.

1.9 We engaged with external stakeholders (industry bodies, UKFIU, law enforcement agencies, MLROs (Money Laundering Reporting Officers), and consultants) to understand current risks and typologies, best practice and challenges in the market, and sought input on how to mitigate the threat of MLTM more effectively.

What we found

1.10 The MLTM threat is continually evolving, and work is required by firms and public bodies to combat MLTM risk. We saw good practice and progress in several financial crime processes and controls across larger and smaller firms. However, further focus and improvement are needed by all to tackle the issues raised in TR19/4, and to support more rigorous mitigation of risks.

Business-wide risk assessment (BWRA)

1.11 Some firms either had not fully considered or had underestimated the financial crime related risks to which they are exposed and insufficiently documented them as part of a tailored BWRA. This led to a lack of understanding across the firm about how they could be targeted by criminals.

Customer risk assessment (CRA)

1.12 CRA processes generally consider a range of appropriate risk factors and are increasingly using weighted factors. Well thought through country risk assessment processes are also more commonplace. However, firms often failed to thoroughly document their CRA methodology or the rationale for the risk rating of a customer where it had been updated or overridden. Not all firms were distinguishing between domestic and foreign Politically Exposed Persons (PEPs) and considering this in their CRA processes.

Know your customer (KYC) and customer due diligence (CDD)

1.13 Onboarding and KYC processes have generally developed to better consider proportionality and customer risk. Firms tend to consider a range of triggers to initiate a customer review or refresh of due diligence. However, there remains an inappropriate reliance by some market participants on other parties in the transaction chain completing appropriate due diligence. Many firms are also not recording and considering the nature, purpose and expected activity on customer accounts.

Governance and oversight

1.14 Firms are developing a tailored approach to formal governance and oversight, to promote oversight and challenge over processes, controls and outcomes. Management Information (MI) reporting on clients onboarded, risk ratings, and surveillance hits has progressed and is generally sufficient to provide relevant updates to management.

Transaction monitoring (TM)

1.15 We found that firms have significant ongoing challenges with TM. Collaboration has improved between TS and TM teams to identify and review potentially suspicious activity. However, most firms have found that using their current automated TM systems in isolation provides limited success in identifying suspicions of MLTM. Automated systems and their alerts are also more often tailored to TS than TM. Firms are not consistently considering how to use TM as part of an integrated process to assist with ongoing monitoring, risk assessment, KYC and record keeping processes to better mitigate MLTM risk.

Investigations and suspicious activity reporting (SAR)

1.16 A significant proportion of firms have limited knowledge of the UKFIU MLTM SARs glossary code. This could impact reporting and wider criminal investigations, and results in a weaker understanding of MLTM risk. SARs reported using the SARs glossary code have increased year-on-year and at a higher growth rate than the full SARs dataset in the same year, but we have seen incorrect use of the code and inconsistent quality of SAR reporting.

1.17 Information sharing between firms continues to be limited. We noted that several firms have not yet considered the expanded information sharing powers in the ECCTA. We encourage firms to use these powers to support the detection and prevention of MLTM.

Training, resourcing and policies and procedures

1.18 Financial crime staff training has become more commonplace at firms. But several firms are yet to tailor training content to their business model, related risks, common red flags and for the different roles that exist in the firm. Resourcing in financial crime functions varies greatly across firms, as does the quality of policies and procedures.

Our expectations of firms

1.19 We expect firms to have robust systems and controls at each stage of the customer and transaction journey. This is essential to make sure there are no 'weak links' that expose participants and the overall transaction to financial crime. Firms must understand the risk posed to, and by, their business, to make sure they take a proportionate risk-based approach to implementing systems and controls. Customer risk needs to be thoroughly understood to provide a meaningful basis for managing the risk and subsequent customer activity monitoring. Suspicious activity should be identified, investigated, mitigated and reported in a timely manner. There should be appropriate oversight, resourcing, training and documentation to support the effective operation of a firm's systems and controls.

Part 1: MLTM risk

Chapter 2

What is Money Laundering Through the Markets (MLTM)?

MLTM is the use of capital markets to launder funds obtained through criminal activity, so that they appear legitimately generated from trading activity.

The MLTM threat continues to rise as criminals become more sophisticated and seek new channels to launder the proceeds of crime. Markets use a variety of complex products and facilitate the movement of vast amounts of capital from different geographical regions with relative ease. It is challenging to accurately quantify money laundering and MLTM to show the threat and trends over time.

Example risks of harm and threats
anonymity of trades
competitive industry and low fees/margins
significant volume, value and speed of transactions
complexity of transaction chains and availability of information
multi-jurisdictional parties
availability of other counterparties / intermediaries where initially refused
complex client corporate structures
identifying beneficiaries of trades
ease of access to products
product complexity/transparency
sophisticated criminals – multiple connected firms and transactions
fraudulent documents and information used for new accounts

Example causes of harm
rapid business growth without appropriate investment in supporting systems and controls
business expansion into riskier models, clients, jurisdictions
under reporting of SARs
pressure to onboard clients quickly
inappropriate reliance on due diligence completed by others
inadequate review and testing of systems and controls
insufficient knowledge and experience of MLRs by staff and SMF holders
under appreciation of risk within a firm

Controls and mitigations

Specific firm risk assessment	Review controls & framework	Thorough due diligence	Front & middle office collaboration
Robust systems & controls	Effective monitoring	Regular & tailored training	Intelligence & suspicions sharing

Challenges faced in reducing MLTM

Weak controls expose whole transaction chain to MLTM risk.	Pre-emptive detection is difficult, as trade activity appears benign by itself.
Siloed front and middle office limit ability to spot and contextualise alerts.	Lack of visibility of whole transaction chain constrains ability to identify ML, including cross border nature of trades and fungibility of funds.
Shallow data prevents identification of UBOs and true sources of ML.	TM systems and controls are not generating relevant alerts/suspicions.
Limited public-private body information sharing to raise awareness, quality and quantity of investigations	Low convictions enable client re-entry.

Part 1: MLTM risk

Chapter 3

Risks and typologies seen in the markets

3.1 Our 2019 thematic review outlined several prominent types of risk (typologies) in capital markets. Firms have told us that these risk typologies have remained fairly static, and some are rarely seen. Many firms determine that customer activity is not necessarily unusual until considered in light of business/money laundering (ML) risks and combined with other KYC information, TM alerts, and other data. Proactive firms have assessed these risk typologies against their businesses to understand which are relevant to them and considered them in their BWRA, product risk assessments, onboarding/KYC, TS and TM processes and controls.

3.2 The following case studies have been provided by firms, industry bodies and market participants to highlight actual, recent examples of risk typologies. They outline the typology and scenario, how they were identified and why they were considered suspicious. These should support firms in reviewing and developing relevant policies, processes, training and staff awareness. Firms should consider the risks these pose in their business, what can be done to mitigate the risks, and how best to identify similar activity and suspicions.

Case Study 1:

Pre-arranged trading in illiquid options or option combinations for the purpose of transferring funds from one account to another.

The client opened a debit spread position at a price that seemed distorted and favourable to the client. This price would not have been available or executable in reasonable market conditions.

The risk was identified through a pre-arranged trading and money pass/compensation trading alert. On investigation, the following risk indicators were identified, the:

- client account was opened and funded a few days before the trade
- account was funded with just enough money to fulfil the margin requirements
- trade was the first trade on the account
- transaction price of the options was out of line with market conditions
- client resided in a high-risk country

Similar activity was detected a few days later from a new account that media access controls (MAC) confirmed was from the same device as before.

Case Study 2:

Free of Payment (FoP) trade to circumvent sanctions.

The client was a non-UK regulated bank, who wanted to transfer shares from a UK to a non-UK custody account, in the name of the same customer.

Sanctions controls and alerts highlighted this transaction and further investigation found that the customer was owned by close associates of a sanctioned individual and had an opaque, non-UK entity within its organisational structure.

Case Study 3:

Account funding where a student received significant cash deposits into their account.

Ongoing due diligence processes identified that the customer received cash gifts from overseas relatives. The firm considered the scale of funding, the involvement of third-party payments, a high-risk jurisdiction, and the risk of money mules.

Case Study 4:

Mirror trading with the same volume/value trading next day that lacked economic sense, to move money from one party to another and legitimise the appearance of funds.

Analysis of the customer's transactional flows showed largely US mega cap stock trading, but with examples of:

- potential mirror trades where buys and sells (with the same volume) occurred on consecutive days
- unexpected trading activity (sudden, large volume trading in stocks not usually associated with the customer account - the entity had only traded one currency stock, then unusually traded in another currency stock in a large amount comparative to total stock volume)

Further investigation discovered that the customer had links to trust or company service providers' (TCSPs) addresses, there had been multiple company name and director changes, links to higher risk jurisdictions for AML/corruption, and negative news alerts.

The firm used red flags seen in this case for training and business/KYC team guidance.

Case Study 5:

Wash trades through simultaneous purchase and sale of shares and index options at identical/almost identical prices by the same direct client, to legitimise the appearance of funds.

The risk was identified through a market abuse surveillance alert, and there were multiple instances over the years involving different direct clients. Due diligence conducted post-trading identified that the trades were executed by 2 different underlying counterparties, but they shared the same beneficial ownership.

Counterparties found in similar examples for this typology were:

- an individual and a legal entity, where the individual is the beneficial owner
- an institutional and a retail client, with the retail client having capacity to trade on behalf of the institutional one
- spouses
- an individual account and a joint account, where one person controlled both

The transaction rationale given was that the counterparties wanted to transfer their positions from one account to the other and maintain the same market exposure.

Case Study 6:

Money pass where an alert was received about Firm A that had traded an oil future contract at a loss, to Firm B. A money pass is a form of wash trading involving money passing between multiple participants to share, clean and conceal money.

The firm reviewed the trading history and identified over 30 instances of trading between Firm A and Firm B in fuel contracts, where Firm A always made a loss.

Case Study 7:

Circular trading in an equity basket, where the client executed a large basket order through an Inter-Dealer Broker (IDB) which included over 30 stocks. Circular trading is a form of wash trading involving multiple participants to obscure the nature of the transaction.

The firm's TS alert highlighted that there was both a buy and sell for the same stock within the basket. Investigation by the firm revealed no valid rationale for the simultaneous buy and sell of the same stock.

Case Study 8:

No economic rationale/out of the money trading where Firm A trades crude oil futures with market participants at the prevailing market price, before trading in the opposite direction with Firm B at a price out of line with the market and beneficial to Firm A. Firm A realises an immediate profit.

The firm found this trading pattern had occurred on 7 occasions across a 3-month period, with Firm B repeatedly losing money.

Case Study 9:

Network of firms where there was substantial trading in non-UK bonds by a network of small UK limited companies that were regulated in the UK. They were moving money from one party to another to legitimise the appearance of funds.

Customer risk factors identified by the firm included:

- the companies' turnovers were small in comparison to trading activity
- minimal content on their websites
- the companies were linked through addresses, auditors and/or employees

The companies involved declined to provide full SoW (source of wealth) and SoF (source of funds) information at onboarding, and stated they were working for unknown family offices. Also, an ex-shareholder of several of the firms involved was sanctioned for fraudulent practices.

Case Study 10:

Parking is transferring assets to another party with the understanding it will purchase them back at a later date.

The firm's TM controls identified a large, short-term loss. On investigation, there was no clear economic sense to this trading activity. The client's CIO (chief information officer) was evasive and aggressive, and similar activity was found when the client's past trading history was reviewed.

The firm shared the case with their other affected global AML teams.

Case Study 11:

Network of accounts where accounts traded short in illiquid options on non-UK exchanges. They were traded at unrealistically high prices with unknown counterparties, either to close them at a lower price or wait for them to expire, so receiving money from the counterparties.

Suspicions were raised as the deposits were small compared with the profits and amounts withdrawn. On investigation, a network of over 20 accounts were linked by similar trading patterns, the same residential addresses, MAC addresses and telephone numbers.

Case Study 12:

Third-party payment to move money between parties and legitimise the appearance of funds.

A UK Prime Brokerage's client was a non-UK regulated asset management firm. The client deals with different bonds and has related corporate action/fees on those bonds. An expected and permissible consent fee was issued by a Russian company on debt. The Russian company is subject to sanctions, and it is prohibited to deal in new debt issued by them after the date of this consent fee. However, the consent fee was not paid by the expected issuer; instead, it was received from another party.

The risk was identified through transaction monitoring alerts triggered by a payment transfer to/from a very high-risk country using a third party. Firm investigation found:

- the actual remitter was in a high-risk, sanction circumvention risk corridor country
- there was no open-source information on the entity or director
- the actual remitter was incorporated shortly after the Ukraine invasion
- the entity purports to be a wholesale exporter (not in line with payment expectations)
- there was no link between the expected and actual remitter

Case Study 13:

Free of Payment (FoP) variation where bonds were transferred between custody brokers of the respective end clients to increase legitimacy of the bond and create the impression of transferring economic value.

Large transfers of non-UK domiciled, Euro denominated, secured bonds were moved through the markets FoP. The issue size was of several €bn, paying a coupon of 5%. Actors held large denominations of the bonds and would be able to justify large payments made to them as coupon payments.

The suspicions this activity raised included:

- the nature and number of the FoP transfers
- there was no economic benefit identified
- the bond was an unusually large size in the context of the bond market
- research into the issuer showed the firm was unable to support the size of the debt
- research into the provider of the security showed the firm was marketing holiday insurance
- there was no market chatter around the time the bond was issued given the issuance size

Risk indicators

3.3 Most firms and industry participants we spoke to told us that risk typologies are often difficult to spot in isolation, due to the challenges indicated in Chapter 2. They are more able to identify suspicious behaviour that corresponded to risk typologies if they consider TM and TS alerts alongside customer information, business risks and recent risk indicators. Below, is a non-exhaustive list of risk indicators for firms to be aware of and consider in training and controls:

- Former customers exited by the firm attempting to re-apply through different legal entities or parties.
- Small and frequent changes in client details. For example, address (and use of residential and TCSP addresses in higher risk jurisdictions); director (and use of nominee directors with higher risk attributes); jurisdiction changes; beneficial owner changes; entity names remarkably similar to larger credible firms; opaque UBO or no public footprint.
- Multiple connections between firms - either business connections, same phone numbers/address/ID photos, similar activity or transactions between them, or personnel moving between firms.
- Bank accounts in a different jurisdiction to where customer is based.
- Transactions involving no ultimate change in beneficial ownership.
- Significant deviation from historical client trading behaviour or profile.
- Customers with overly complex structures without clear rationale.
- Customers that deposit and withdraw funds in quick succession.
- Unusual or unexpected foreign exchange trades.
- Uneconomic or irrational trading strategies.
- Settlements or payments to/from third parties that have no apparent connection with the transaction or customer.
- Material inconsistencies between CDD and Companies House information.
- Same counterparties on each side of the trade.
- Subscribing into long term funds but redeeming within weeks, or subscribing for further shares whilst also looking to redeem.
- Multiple payment methods/cards, including attempts to directly fund bank and trading accounts from third parties, or failed direct debits.
- Deposits exceeding salary or turnover expectations.
- Accounts linked by devices, for example, PC MAC addresses or mobile phone handset IMEI (international mobile equipment identity) numbers.
- Abnormal funding patterns. For example, no trading between deposits and withdrawals; minimal trading before balance is withdrawn; small positions compared to both size of account balance and normal market trading sizes for instrument; failed or aborted funding and withdrawal transactions; significant funding in a short period without rationale.
- Use of complex and structured products and patterns to launder money, whereby the client is not waiting until maturity, or is content with making a loss on the contract at maturity.

Part 1: MLTM risk

Chapter 4

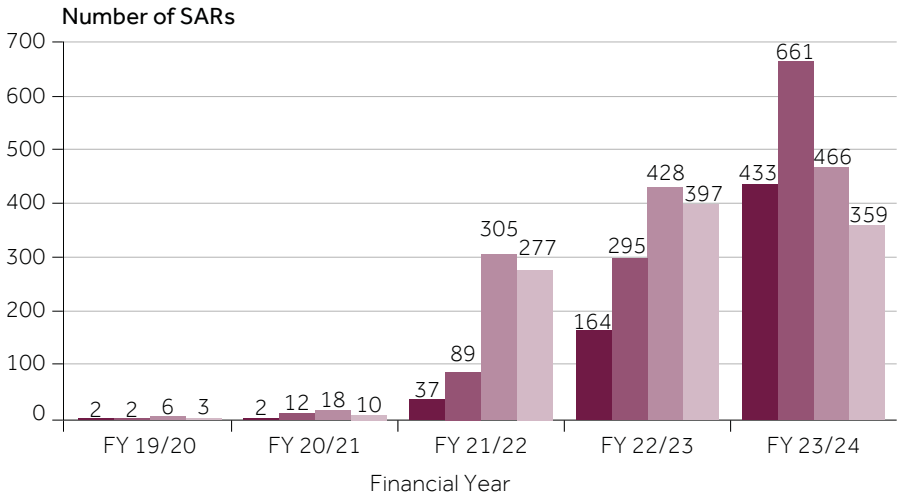
How suspicions of MLTM should be reported and SAR reporting trends

4.1 The 'XXMLTMXX' SAR glossary code was officially supported and promoted by the UKFIU in May 2021 for reporting suspicions of MLTM. The UKFIU states that 'MLTM in its simplest terms is ML taking place within capital markets in which shares, derivatives, bonds and other instruments are bought and sold. The glossary code should not be used for market abuse such as insider trading or market manipulation unless specific reference is made to the subsequent laundering of the proceeds of these crimes'.

4.2 The UKFIU's resources to support firms in understanding SAR reporting include: SARs intro and guidance; SAR reporter booklets which provide case studies where SARs have helped investigations; Guidance on submitting better quality SARs; SARs in Action magazines; SARs Annual Statistical Report 2023.

4.3 We commissioned a Statistical Brief from the UKFIU on SARs containing the MLTM glossary code, highlighting trends and pattens within those SARs as of 30 August 2024. While Figures 1-3 show a large year-on-year increase in the number of SARs reported using the MLTM glossary code, our firm assessments have shown firms using the MLTM glossary code incorrectly[1] (see Chapter 12). Wider analysis has not been completed on the overall quality of MLTM SARs reported, nor the potential link between increased detection or reporting of MLTM SARs and increased money laundering.

Figure 1: Number of SARs relating to MLTM, by quarter and financial year (FY) between 01/04/19-31/03/24 (UKFIU Statistical Brief as of 30 August 2024)



FY Total	13	42	708	1284	1919	3962
% change in MLTM SARs submitted		223%	1582%	81%	49%	
% change in all SARs submitted		30%	21%	5%	2%	

Q1 (Apr – Jun) Q2 (Jul – Sept) Q3 (Oct – Dec) Q4 (Jan – Mar)

1 The UKFIU has not conducted any analysis on the quality of SARs using the MLTM glossary code, and makes no comment on whether or not the glossary code has been used correctly.

Figure 2: Split of DAML and intelligence only SARs relating to MLTM between 01/04/19-31/03/24 (UKFIU Statistical Brief as of 30 August 2024)

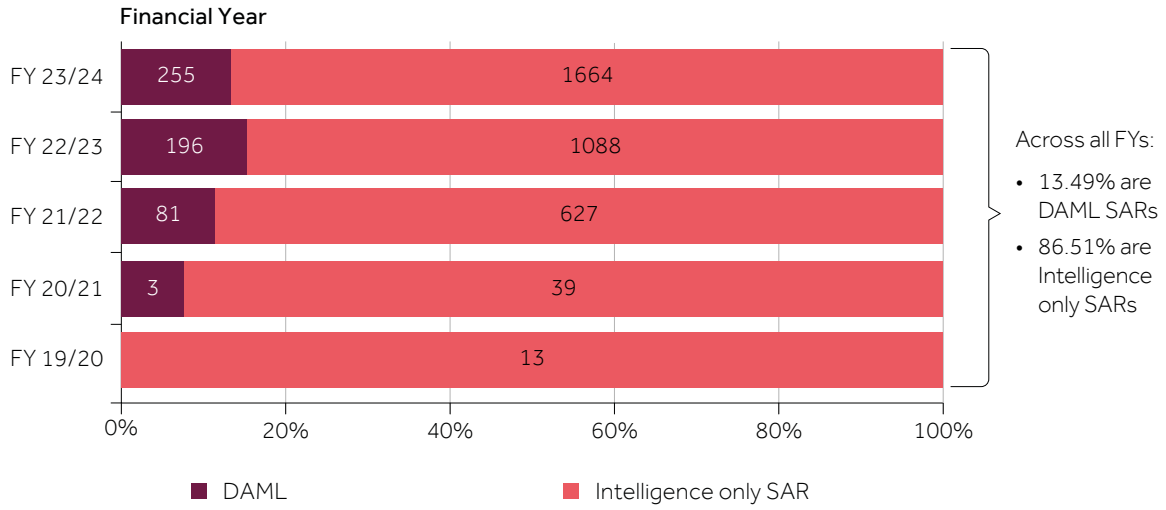
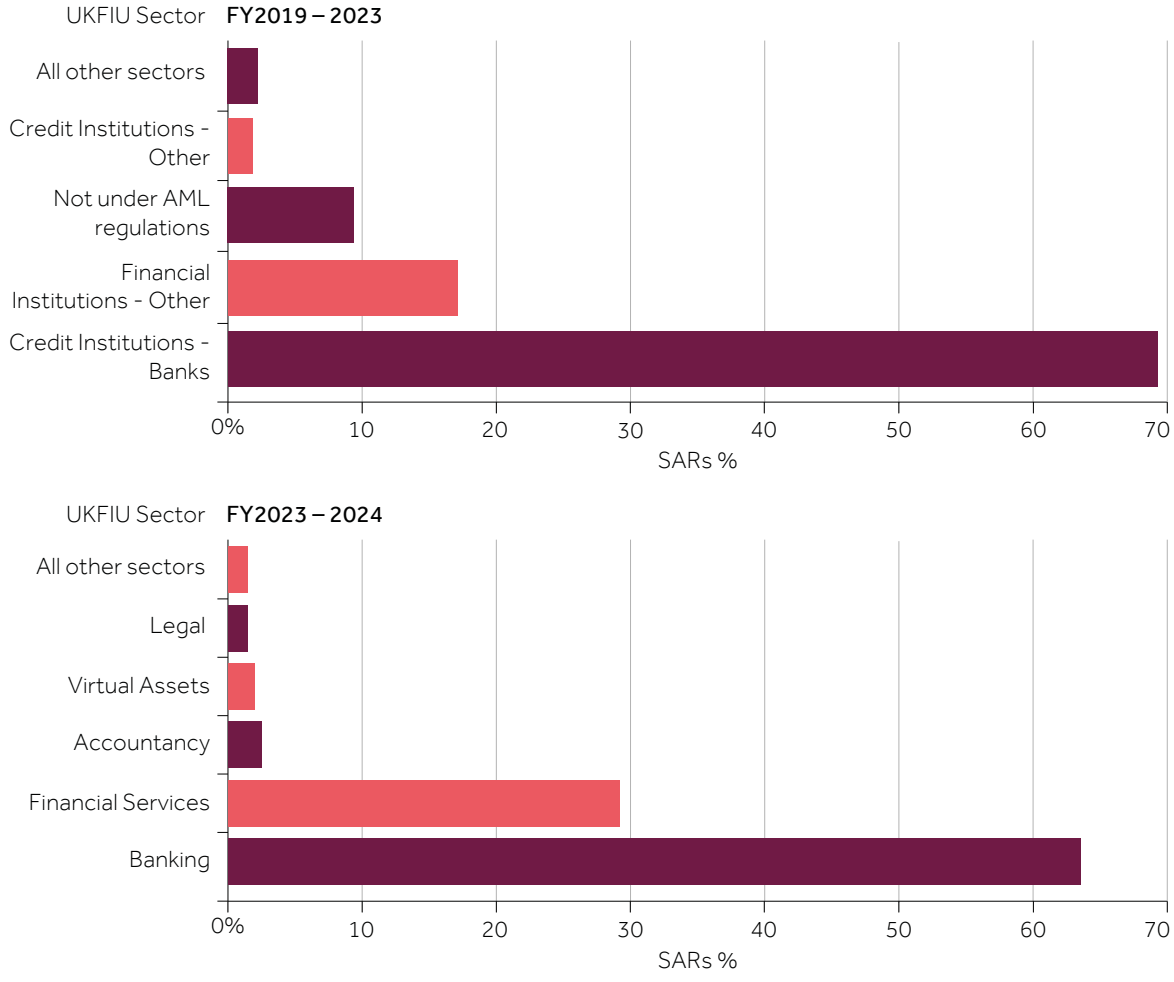


Figure 3: SARs relating to MLTM between 01/04/19-31/03/24 by UKFIU sector, as a percentage. ('Sectors' were amended for FY2023/24 and all reporters re-registered; Wholesale Brokers categorised under multiple 'sectors' during FY2019-2023 and under 'Financial Services' during FY2023/24) (UKFIU Statistical Brief as of 30 August 2024)



Part 1: MLTM risk

Chapter 5

Wholesale brokers and the risks and concerns they pose

5.1 Wholesale brokers primarily act as agents and do not take proprietary trading positions. They play a valuable role in sourcing liquidity for their clients and providing market information. They do this by matching buyers and sellers in markets and in the case of smaller brokers in particular, by providing market access to clients that banks consider uneconomic to service. They also facilitate price discovery and offer bespoke trading solutions.

5.2 Wholesale brokers mainly service institutional clients and, typically, larger clients such as wholesale banks, investment funds, corporate finance firms, family offices, and some high net-worth individuals.

5.3 Their core activity is providing arranging and execution services in equities, bonds, commodities, derivatives or FX to institutional clients in the banking, asset management, trading, prime brokerage and corporate sectors. Outside of the larger interdealer brokers that hold the majority of market share, the rest of the market consists of firms of varying sizes with a notable number of firms that specialise in niche markets or products, such as equity markets, some oil derivatives or crypto assets. See Figure 5 for an illustration of the instruments that are traded in the UK through wholesale brokers.

5.4 Larger brokers often operate their own venues (MTFs (multilateral trading facilities) or OTFs (organised trading facilities)) and may also offer custody, clearing, research, payment and corporate finance services, setting themselves apart from the majority of the sector. They tend to use the 3 main broking models: name give-up, exchange give-up and matched principal.

5.5 There are approximately 280 wholesale broker firms regulated in the UK, with combined total 2023 revenues of over £24bn (FSA030 P&L reporting).

Figure 4: Size of wholesale brokers market represented by percentage of brokers split by 2023 revenue bands (FSA030 P&L reporting data as at 23 July 2024)

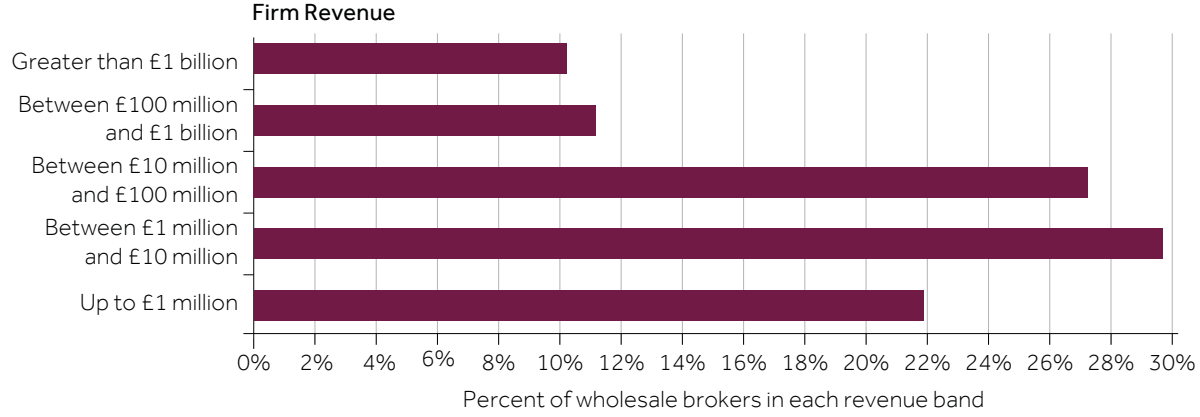
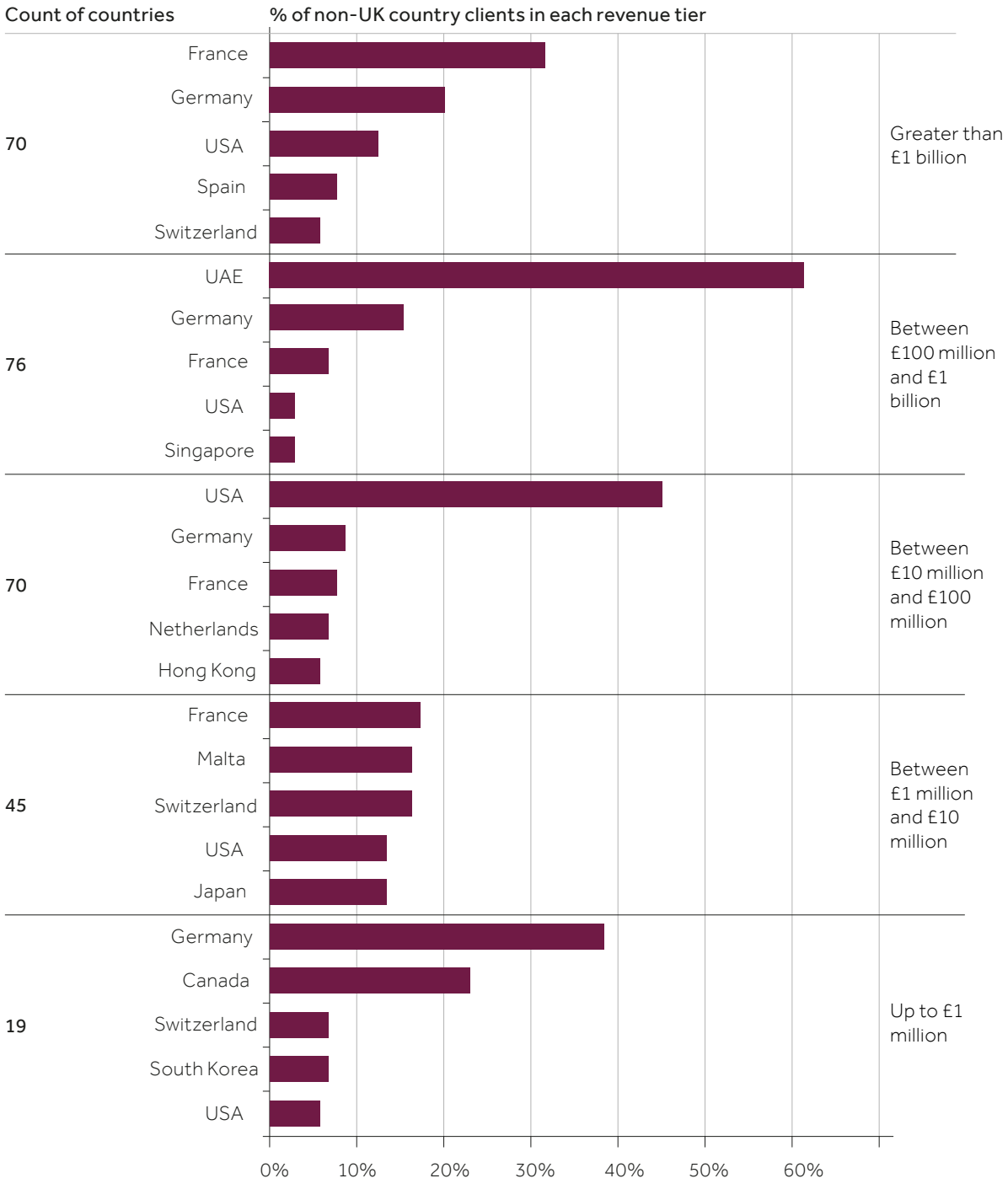


Figure 5: Instruments traded each year as a percentage of total notional GBP* and total transaction count for all wholesale brokers (MiFID Transaction Reporting as at 23 July 2024 for period ending 30 June 2024)

*Total notional executed: the notional value of all transactions which pass through all wholesale brokers

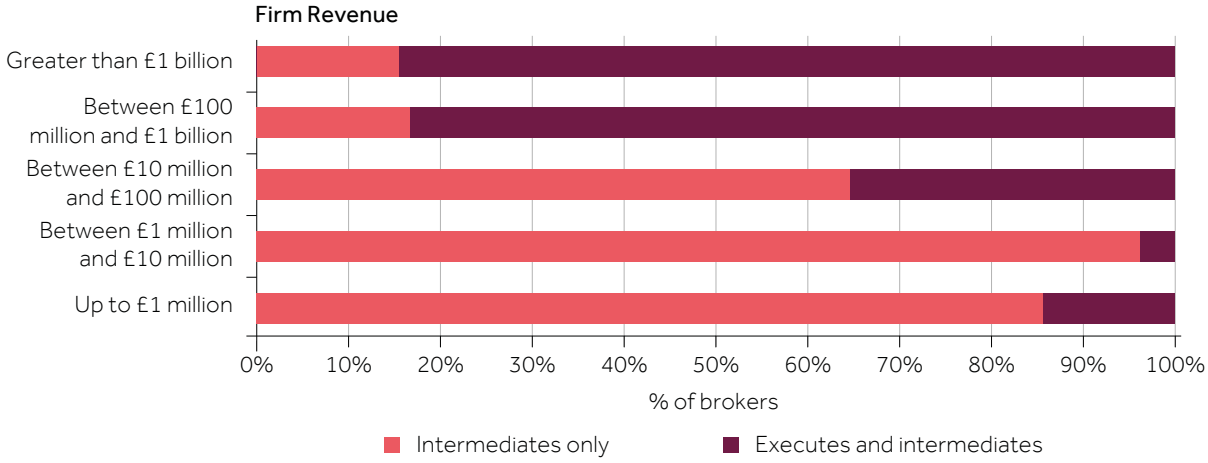
Figure 6: Top 5 countries where trades appear to originate from in Jul23-Jun24 MiFID transaction reporting data, split by revenue bands, for all wholesale brokers (excl. UK). Data as at 23 July 2024.



5.6 Brokers play an important role in maintaining the effectiveness of UK wholesale markets. Their position in those markets, the wide variety of countries that trades originate from (see Figure 6) and the level of discretion they can have in bringing transactions together means they can have a significant impact on the integrity of markets. This also makes them vulnerable to exploitation for MLTM purposes.

5.7 Capital markets may be used to disguise the origins of financial gains from criminal activities. For example, customers purchasing securities or entering into financial contracts using illicit funds and selling or exiting those contracts. Introducing or agency brokers handle customer interactions and pass orders to clearing brokers, who may lack complete visibility of the underlying customers. Global flows, speed of transactions, ease of converting holdings into cash and complex transaction chains are potential vulnerabilities.

Figure 7: Wholesale brokers role, identified through their position in transaction chains, as a percentage of all wholesale brokers in each revenue band (MiFID Jul23-Jun24 Transaction Reporting data as at 23 July 2024)



5.8 In our Dear CEO letters (2019 and 2023) and through our supervisory engagement, we noted the following financial crime related areas of concern across the wholesale broker sector:

- Limited governance, accountability and poor culture.
- Lack of senior management engagement in identifying financial crime risks.
- Failure to understand financial crime risks of wholesale brokers.
- Lack of understanding of responsibilities for mitigating and managing risks.
- Underinvestment in systems, controls and training to manage risk.
- Control functions are not properly resourced or empowered to effectively challenge the business.
- Misperception that firms that are not authorised to hold/control client money or custody assets under CASS (client asset sourcebook) permissions have limited to no responsibilities for mitigating financial crime.

Part 1: MLTM risk

Chapter 6

How we did this work and how we selected firms for this review

6.1 We completed detailed firm reviews to assess the financial crime systems and controls on a range of topics listed in 6.5 and to:

- Understand how MLTM issues, themes and risks have changed since our 2019 thematic review.
- Consider the issues, risks, challenges and suggestions that external stakeholders told us about.
- Review firms' systems and controls issues and themes from recent and previous supervisory work.
- Assess firms' systems and controls to understand current issues, themes, and areas of good and poor practice.
- Analyse how firms have understood and used previous FCA reviews and Dear CEO letters to enhance their systems and controls.

6.2 Through rigorous data analysis, we selected a sample of wholesale broker firms based on the following criteria:

- Firms of different sizes, determined for example through annual revenue, number of customers, volume of transactions, etc.
- Several of the different business models that exist in the wholesale broker sector. For example, considering service offering to customers, engagement with other market participants, client money permissions, and jurisdictional reach.
- Previous supervisory work and information held that indicated potential firm issues or good practice systems and controls.
- Perceived financial crime risk at the firm, indicated through firm information held and risk indicators observed through a firm's annual financial crime report (REP-CRIM).

6.3 We conducted detailed reviews on these firms, and believe they reasonably represent the variety and diversity of wholesale brokers across the sector. Our sample of firms represented 8% of the yearly notional value of all transactions that pass through all wholesale brokers (2023 MiFID transaction reporting) and 21% of market share based on the yearly revenues of all wholesale brokers (2023 FSA030 P&L reporting).

6.4 Our detailed assessments on firms' systems and controls included reviewing policies and procedures against regulations and industry guidance. We then tested the appropriateness and operational effectiveness of firm processes by analysing customer files, SAR submissions and associated investigations, and assessing the level of knowledge held by relevant staff.

6.5 In Part 2, we document our findings, case studies and good/poor practices identified for each of the financial crime topics assessed. Those being BWRA; CRA; KYC and CDD checks; governance and oversight; TM; investigations and SARs; and training.

Part 2: Findings

Chapter 7

Business-wide risk assessment (BWRA)

What this is

7.1 A thorough understanding of financial crime risks is crucial so that firms can apply proportionate and effective systems and controls to manage and mitigate such risks appropriately, in line with Regulations 18 and 18A of the MLRs. Guidance from paragraph 2.2.4 FCA Financial Crime Guide, JMLSG (Joint Money Laundering Steering Group), and FATF (Financial Action Task Force) is available to support firms.

What we saw

7.2 We noted firms using a variety of approaches towards completing a BWRA. Business size was not a determining factor in whether firms had a holistic BWRA. Some firms failed to tailor their risk assessments to their specific businesses and/or included generic risks which may not be relevant. Common characteristics of effective BWRAs included consideration of specific risks related to the business model, quantifying and evaluating residual risks, and explaining steps taken to mitigate and manage risks within their appetite.

7.3 During our review, we saw that many firms failed to document their BWRA appropriately and did not show how it feeds into other business processes, controls and decision making. We also found that BWRAs often did not identify the scenarios that would trigger an updated assessment and did not adequately consider Terrorist Financing (TF) and proliferation finance (PF) risks.

7.4 We found several instances where senior management was unable to adequately explain the financial crime risks facing their firm, and how these were mitigated by the systems and controls in place. These firms were found to have ineffective BWRAs.

7.5 We saw some instances where firms prohibited services to entire groups or types of customers without appropriate rationale, consideration and justification. Firms should adopt a risk-based approach and implement suitable controls, rather than wholesale de-risking without sufficient rationale.

7.6 We noted that business risks were often too broadly defined and assessed. This could lead to a lack of understanding across the firm on how they could be targeted by criminals. All staff in a firm need to be alert to, and collectively manage, risks.

7.7 The following case studies show how some firms have approached their BWRA. Firms should compare and contrast them with their own BWRA.

Case Study 14

The firm's BWRA documents a qualitative and quantitative assessment of the business risks. The BWRA contains firm-specific analysis of a variety of inherent risk factors that include exposure to predicate offences, operating environment, and PF.

An impact and probability scoring of 1-5 is assigned to each risk factor and sub-factors to create inherent risk scores. Total inherent risk divided by total risks is calculated to produce an overall inherent risk score that the firm equates to a level of exposure to ML and TF. Key risks, mitigation and actions taken are also in the firm's BWRA.

The firm's residual risk score is calculated by multiplying overall inherent risk by perceived strength of controls to conclude that residual risk exposures to ML/TF (terrorist financing) is 'low'.

The BWRA outputs are compared to the firm's ML and TF appetite thresholds to determine whether they are operating within their risk appetite.

Case Study 15

The firm's BWRA uses a qualitative and quantitative assessment of key business risks, including reputational and financial/regulatory risk, to derive an inherent risk score.

The quality of controls and mitigating strategies are assessed to calculate an average inherent risk score, which is used to derive residual risk scores.

The assessment and scoring are validated with front office before proceeding through governance forums. Heatmaps are produced showing residual risk scores for all key business risks and how they correlate to AML, ABC (anti-bribery and corruption) and sanctions topics.

Our expectations of firms

7.8 Firms should document and assess the financial crime risks to which they are exposed as part of a risk-based approach to implementing robust systems and controls.

Good practices identified

- Quantitative and qualitative risk assessment of the specific business and services offered by the firm – and across each legal entity where appropriate.
- Inherent risks, mitigating factors, controls and residual risks are properly considered and documented.

- Financial crime related risks and typologies are used to assess the risks of new products and services.
- Annual red flag analysis covering relevant risk typologies is mapped against the products offered by the firm.
- Analysing risk typologies against business activity to determine relevance and applicability, feeding typologies into inherent risk scores, and assessing whether sufficient controls are in place to mitigate the risks identified by the typologies.
- Supporting risk registers for each area of the business.

Poor practices identified

- BWRA is not tailored to the specific nature of the firm and its business.
- No defined methodology for assessing known and emerging risks.
- No consideration of TF and PF risks in the BWRA.
- Lack of consideration on how the BWRA feeds into overall financial crime decisions and controls.

Part 2: Findings

Chapter 8

Customer risk assessment (CRA)

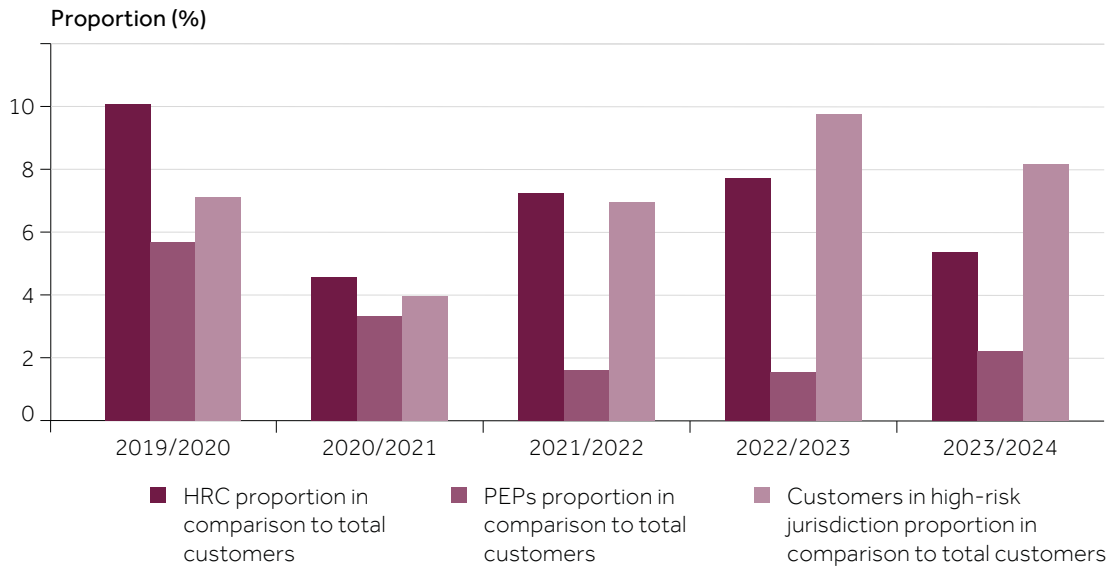
What this is

8.1 Firms are responsible for conducting risk assessments of their customers in line with Regulation 28 (12 and 13) of the MLRs and further support is in paragraph 3.2.3 of the FCA Financial Crime Guide.

What we saw

8.2 Around 190 wholesale broker firms have submitted their annual financial crime report (REP-CRIM) for 2023/24 (as at 1 October 2024). They collectively reported that 56% of their customers are located in the UK, 19% from EEA & Switzerland, 9% from Asia, 6% from North America, 4% from Middle East and Africa, 2% from elsewhere in Europe, 2% in Central America, 1% in Oceana and 1% in South America.

Figure 8: High-risk rated customers (HRC), PEP (politically exposed person) and high-risk jurisdiction customers as a proportion of total wholesale broker customers (REP-CRIM data as at 1 October 2024. See REP-CRIM guidance for further data definitions).



8.3 We noted various examples of how geographical risk is assessed in CRA processes – see Case Study 16 for a good illustration. Some firms only considered changes to geographical risk during the customer periodic review. This could result in the customer risk rating not accurately considering interim information, which could impact risk and result in a failure to act. Firms should consider the events that would trigger a review or CRA update.

Case Study 16

The firm uses a third-party country ratings tool to calculate risk-weighted scores for each country that are then used to derive CRA ratings. The firm allocates a rating of high/medium/low to the risk scores generated by the tool. The firm then manually and regularly checks the tool to identify if a country risk has changed.

In considering the geographical risk for a specific customer, the country of registration, country of operation, and country of domicile of any UBO are all taken into account.

The country risk factors used in the tool include the following, in order of weighting:

- ML/TF risks
- international sanctions
- corruption risks
- global initiative criminality index
- global initiative resilience index
- EU tax blacklist
- offshore finance centre

8.4 Most firms that we observed considered a variety of risk factors and several firms weighted their calculations. Some firms showed clear thought process and consideration of particular risk factors relevant to their business. See Figure 6 in Chapter 5 for an illustration of customer geographical risk at all wholesale brokers.

8.5 Most assessed firms failed to document the CRA methodology in their policies or procedures. We found instances where all 'name give-up' business model clients (off-exchange deal between parties at mutually acceptable terms, before passing names to each client so that they can conclude the transaction bilaterally) and regulated entities were automatically assigned as low risk and simplified due diligence (SDD) carried out, regardless of other risk factors. We also noted an instance where individual CRAs had not been completed at the time of our visit. The firm is now rectifying this. Another observation was the determination of customers' risk rating upon completion of due diligence rather than using the CRA to determine the level of due diligence to be completed. We also saw firms basing the CRA solely on customer jurisdiction and limited consideration of other risk factors or information received.

8.6 Few firms adequately documented an appropriate rationale for the risk rating of a customer. This was particularly the case where updated risk factors or trigger events, management overrides, and periodic reviews had taken place. Evidence of appropriate escalations, decisions taken, and any quality assurance checks completed were often not evident.

8.7 A limited number of firms distinguished between domestic and foreign PEPs in line with Regulation 35(3)(A) of the MLRs when completing the CRA – see the FCA's wider review and the FCA's guidance for information.

8.8 Case Study 17 illustrates a reasonable approach to calculating risk ratings.

Case Study 17

The firm has a spreadsheet that is completed by the onboarding team. It contains detailed questions and risk scoring for the following categories: product and service (10%); customer type (20%); customer industry (10%); geographical (30%); relationship structure (5%); adverse media and PEP (25%).

The total risk score per category is multiplied by the weightings above to create a total risk score. This risk score aligns to a high/medium/low CRA rating and determines the level of due diligence to be completed.

The spreadsheet also alerts the reader if they need to escalate to the MLRO for approval and has a chapter for manual overrides and its rationale. It also prompts the user to consider the presence of other risk factors and information that would require additional action to be taken.

Our expectations of firms

8.9 Firms should have a formal, robust method for considering, assessing and determining customer risk, so as to implement proportionate and effective financial crime processes and controls.

Good practices identified

- CRA process considers a variety of financial crime related risks specific to the business.
- Appropriate consideration given to factors that present higher risks, weighting risk factors, and documenting how risks are mitigated.
- Clear audit trail of customer risk rating overrides and rationale.
- Clear methodology for assessing country risk on an ongoing basis.

Poor practices identified

- CRA scores predominantly based on one risk factor, for example, jurisdiction.
- Waiting for periodic reviews or file refreshes to update risk ratings where new information and changes to risks have been identified.
- CRA methodology is poorly documented in procedures.
- PEPs considered high-risk as a starting point, regardless of whether they are domestic or foreign PEPs, resulting in a lack of appropriate and risk-based EDD.

Part 2: Findings

Chapter 9

KYC and customer due diligence (CDD)

What this is

9.1 Firms are responsible for understanding their customers and completing appropriate customer due diligence in line with Regulation 28(1) of the MLRs.

What we saw

9.2 Our review highlighted some 'broad-brush' approaches that led to undesirable outcomes. Examples are in the poor practices chapter. A firm's documented approach to CRA, risk levels assigned, and levels of CDD carried out will directly impact the understanding of customers and the risks posed, as well as affecting the risk profile of the firm.

9.3 We found instances of firms using in-house electronic onboarding platforms where onboarding data collection and recording is standardised. These are also used for updating KYC records, triggering reviews and they sometimes automatically calculate risk ratings. They often provide an audit trail of activity, tasks for the processor to follow, guidance, assessment/commentary, repository of documents and a record of sign-off.

9.4 However, a significant proportion of firms assessed do not record their assessment of the nature and purpose of the account and expected account activity (transaction size, frequency) during KYC. This limits firms' understanding of their customers and ability to carry out TM and identify suspicious activity for review and effective SAR reporting.

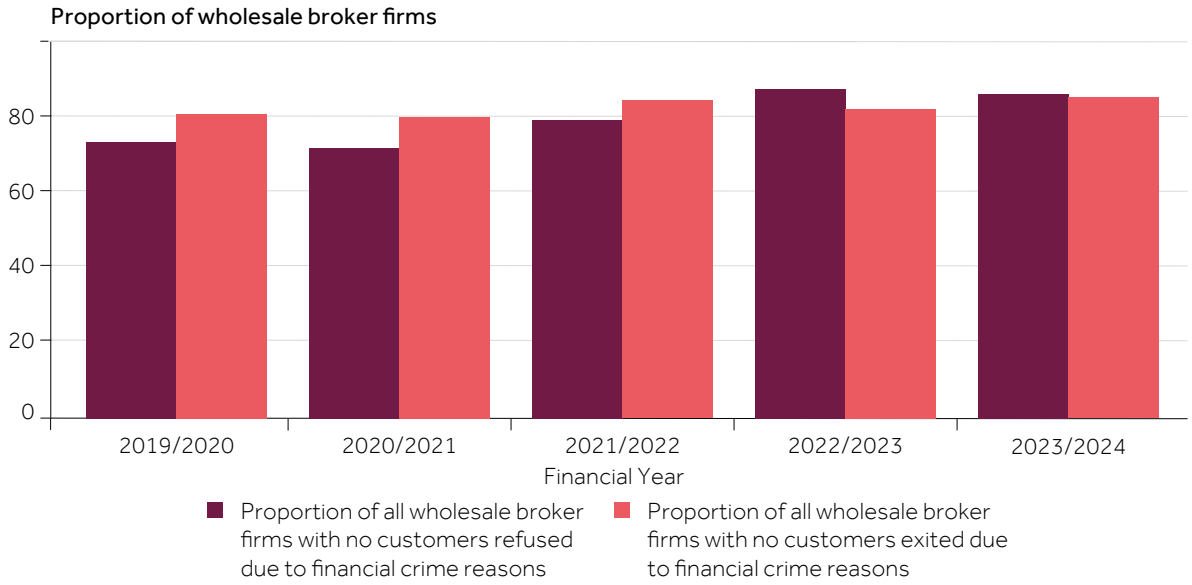
9.5 All firms assessed used third-party tools to conduct PEP, sanctions and adverse media screening checks. Detailed customer information is entered into the third-party database during onboarding screening. The database is automatically screened periodically, triggering alerts for review by firms as potential hits are identified. Around 73% of all wholesale brokers use automated screening and more than 91% of them perform repeated screening (2023/24 REP-CRIM data as of 1 October 2024).

9.6 We saw a clear difference between firms in how they used the customer risk rating to determine the level of CDD. Some firms determined the level of CDD and checks to be completed solely based on their understanding that their customers and business models were predominantly low risk, rather than CRA ratings. Other firms clearly articulated and documented the appropriate levels of CDD to be carried out, documents to be requested and rationale for doing so. These firms tailored CDD to perceived risk, the type of customer and the capacity that the customer is acting in.

9.7 Our review revealed some firms onboarding customers through their non-UK entities, but over time those customers appear on their UK registers. Often no further CDD is either considered or completed to ensure UK requirements are met, and to understand the purpose of the customer becoming a UK business customer.

9.8 We found low numbers of customers being refused accounts for financial crime related reasons. This does not necessarily indicate an issue. However, firms should review processes to make sure they are operating effectively, and at the same time make sure customers are treated appropriately when accounts are closed. This observation is echoed in REP-CRIM returns – see Figure 9.

Figure 9: Proportion of all wholesale brokers reporting no customers refused and no customers exited for financial crime reasons. 27 wholesale broker firms have no customers refused and no customers exited for all 5 years (REP-CRIM data as at 1 October 2024)



9.9 We saw that firms use a cycle of periodic customer reviews most often determined on a 1/3/5-year basis according to customer risk level. Several firms trigger a KYC refresh based on a SAR having been raised on the customer; PEP/sanction screening and TS/TM alerts being generated; new information or adverse media made available; new products being offered; change of circumstances or details of the customer; and following regulatory and industry updates.

9.10 We support firms' reliance on others' due diligence processes where this is appropriate. This increases the overall efficiency of the process. However, our review suggests some firms are relying on others where this is not permitted under the MLRs (Regulation 39 of the MLRs). We were concerned with the assumptions made by firms that others in the transaction chain will have done appropriate due diligence. We noted instances where firms were informally depending on other counterparties in the transaction chain completing appropriate CDD or on the customer being a regulated entity in a jurisdiction of equivalence. The perception that customer ML risk is lower with exchange trading as exchanges have better visibility is unfounded. Exchanges complete CDD on members but do not (and are not expected to) complete CDD on the underlying customers. This informal dependence is often inappropriately used as justification for customers, transactions and the business being low risk. Unless appropriate reliance

agreements are in place, all regulated firms are responsible for completing their own appropriate CDD and fully understanding and mitigating the level of financial crime related risk posed by their customers. Firms should also make sure that reliance agreements, where used, include obligations to provide CDD information promptly and that sufficient oversight is maintained.

9.11 We assessed several customer files and noted:

- Assessment of documents received, and determination of customer risk is often not recorded.
- Account review and sign-off is not always formalised and documented.
- Inconsistencies in the completion of ID&V (identity and verification) and SoW/SoF checks. Checks are often insufficient and lack appropriate evidence and assessment.
- TM completed and actions taken are not visible in customer files.
- Periodic reviews are hastily completed and rarely look holistically at all the information held on the customer.

9.12 We saw the following firm onboarding scenarios, which may provide training and awareness opportunities for firms.

Case Study 18

The firm received an automated alert that client funds received were not in line with the customer's stated expectations indicated at onboarding.

The firm's MLRO had discussions with the institutional client's MLRO to understand the rationale and likely future activity, so that KYC information could be updated.

Case Study 19

The firm's onboarding team internally escalated the onboarding request due to a high-risk jurisdiction. The entity was unregulated and providing proprietary, cross commodity and systematic trading based on signal generation.

The firm reviewed the KYC information held and identified the following red flags:

- inconsistencies between KYC information held and information on the company register and company websites
- complex and opaque ownership structure
- negative news
- TCSP addresses
- high-risk customer jurisdictions involved

Our expectations of firms

9.13 Firms must identify and collect relevant customer information to make sure they have a thorough understanding of the customer and the financial crime risks associated with the customer relationship. This is important for completion of KYC checks, to manage risk factors, and to provide a meaningful basis for subsequent customer activity monitoring.

Good practices identified

- Independently verifying ID, adverse media, and documents received where possible.
- Getting relevant information to enable an assessment of the customer's systems and controls (for example, policies, information on the firm and the regulatory regimes they operate in).
- Defined risk-based trigger approach for reviewing and monitoring accounts.
- Matrix of AML requirements (for example, documents to request, checks to complete, rationale) per type of institutional customer and by customer risk rating.
- 4-eyes checking of onboarding activities before a customer is approved.
- Checklist of tasks to complete during a customer periodic review and refresh.
- Relationship manager completing checks and understanding the client, to filter out any business that is against risk appetite before progressing to onboarding.
- Re-completing onboarding KYC process after a period of non-trading.
- Firm to firm discussions to raise queries on documents, consider changes in risk profile, and understand customer activity.
- Identifying if the customer is acting as agent or principal and tailoring CDD accordingly.
- Assessing MI on upcoming periodic reviews to make sure resourcing is available.
- Firm's compliance staff met with the client's compliance officers and other Senior Executives at the client's offices to discuss and understand their systems, controls, processes and procedures as part of the KYC process.
- Requesting a Wolfsberg questionnaire, where appropriate, to support due diligence processes.
- A firm's SoW questionnaire was structured to guide the case handler through the range of potential evidence that may be required in the following areas: 1. Employment details (CV, payslips, tax returns, accounts, contracts, bank statements); 2. Business income (company accounts; proof of ownership); 3. Inheritance or gifts (court documents, bank statements); 4. Sale of property or investments (legal documents / contracts, bank statements); 5. Other (independently verified documents).

Poor practices identified

- The nature and purpose of the account, expected account activity (size, frequency of transactions) and payment methods are not understood and documented.
- Lack of understanding and documentation of the institutional customer's risk appetite, its controls, and the risk profile of its customer base.
- TM, TS and SARs are not considered in KYC and monitoring processes.
- Requirement to identify and report material discrepancies under Regulation 30A of the MLRs is not included in procedures.
- No evidence of assessment and challenge on information received from customers, for example, on SoW/SoF checks.
- Account approval audit trails and rationale are not stored on customer files.
- Customers onboarded for non-UK entities in the group, but then added onto the UK entity register later without due consideration to the customer's purpose and any additional due diligence that should be carried out.
- Give-up or regulated clients subjected to SDD (simplified due diligence) irrespective of risk factors.
- Backlog of periodic KYC reviews remain unresolved for a long time.
- Guidance on red flags is not documented in procedures.
- No evidence maintained of relevant and appropriate screening being completed.
- Applying EDD (enhanced due diligence) to all customers regardless of risk.
- No recorded assessment of screening checks undertaken and documents received and reviewed, and insufficient rationale to show the firm's acceptance and onboarding of the customer.
- No documentation of actions taken following a change in circumstances.
- Approach to periodic reviews is not risk based, for example, basing on alphabetical order of customers.
- Potential connections between parties are not considered during KYC processes.
- SoW/SoF determined on a case-by-case basis instead of a defined process.
- Screening is completed after the customer has been onboarded.
- Completing limited or inconsistent ID&V checks to support the KYC assessment.
- Customer inconsistencies are not followed up, for example, different email addresses, different companies stated, income on bank statement differs to application form.

Part 2: Findings

Chapter 10

Governance and oversight

What this is

10.1 Firms are responsible for making sure appropriate governance and oversight mechanisms are in place to support a firm's systems and controls. Further support is in paragraphs 2.2.1-3, 2.2.7 and 3.2.1-2 of the FCA Financial Crime Guide.

What we saw

10.2 Many firms recognise the importance of strong governance and oversight to support the effectiveness of their systems and controls. We noted firms engaging with customer onboarding committees and risk committees to discuss risks, decisions and challenges. They have also tabled risk discussions as a standing agenda item for Board meetings. Committee quorums are often used to ensure wider business representation and participation in decision making.

10.3 Our review found MI reporting is used to inform and drive senior management decision making, as well as supporting the business and its systems and controls. Firms with larger customer bases often produce monthly packs that combine:

- AML monitoring (customer rejections, new accounts by risk rating, top 10 high-risk customers, screening figures, periodic review backlog, SARs, breaches, QA/QC (quality assurance /control) results)
- TS/TM joint monitoring (alerts, updates)
- regulatory monitoring
- project updates

10.4 Most firms had well-constructed and detailed MLRO reports.

10.5 Several firms had considered and documented their formal approach to independently completing a QA/QC process – including sample checking by compliance, internal audits, external reviews. These firms were aware of gaps identified in the control framework and their financial crime strategy and remedial actions planned. However, other firms were unable to show awareness of any gaps or areas for improvement in their systems and controls.

10.6 We noted that smaller firms often encountered challenges with assigning SMF (senior management function) roles and ensuring independence. Dual SMF roles are sometimes held by individuals which could impact the effective execution of AML/financial crime duties and processes. Some SMF16 and 17s lacked the expected understanding of compliance, MLRs or the firm's actual business. In one firm, conflicts of interests had not been appropriately considered and managed, where individuals held Head of Compliance/Partner (SMF16/27) and MLRO/COO (SMF17/24) roles.

10.7 One firm's Board discussed onboarding customers from a new country and the impact on the firm's risk profile. The Board conditionally approved onboarding of customers from this country, to appropriately manage the firm's risk profile.

Our expectations of firms

10.8 While smaller firms often take a flexible and commensurate approach to formal governance and oversight, financial crime issues must be formally discussed, decisions recorded, and appropriate oversight and challenge given over processes, controls and outcomes.

Good practices identified

- Formal governance processes to discuss, review and approve customer onboarding.
- Monthly reporting of onboarding, TM, TS and other ML data statistics for staff and senior management awareness and decision making.
- Independent QA/QC undertaken on policies, procedures, controls, case reviews.

Poor practices identified

- Arrangements not in place to make sure possible conflicts of interest are managed, independence maintained, and duties carried out effectively for SMF role holders.
- Insufficient ML/financial crime knowledge and awareness held by SMF role holders.
- Management discussions, decisions, approvals and actions are not documented.

Part 2: Findings

Chapter 11

Transaction monitoring (TM)

What this is

11.1 The MLRs require firms to conduct ongoing monitoring of a business relationship, including scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the SoF).

What we saw

11.2 During our review, we noted some firms finding it difficult to identify suspicious activity due to:

- Lack of transparency and visibility of transactions (illustrated in Figure 10).
- The volume of trades compared to scalability of solutions and firm resources.
- Low numbers of MLTM specific TM controls and alerts.
- The scale of false positives that are sometimes generated and the firm's ability to investigate the alerts.

Figure 10: Illustrates a simple, hypothetical transaction and highlights the potential complexity involved in identifying, understanding, monitoring and mitigating risk in the whole transaction chain by all participants. The UK is an international hub, so trades with international parties are common and there may be little visibility of who all the 'clients' are. Additional parties and firms providing services will make this task even more challenging. The inclusion of big banks, for example, may provide false comfort or legitimacy to the transaction and parties involved.

11.3 Many firms assessed use both automated and manual processes to complete TM. Some firms are developing in-house 'reg-tech' solutions to align more effectively with their business, products and customer risk profiles. The larger firms that we saw appeared more advanced in the use of technology-based solutions. Firms that use only manual TM processes may face challenges with the assessment and determination of relevant TM rules and scalability of such an approach, as well as with appropriate resourcing to review activity. Automated processes are often more focused on TS than TM, and TM alerts relevant to capital markets remain limited.

11.4 Our review highlighted that monitoring transactions in isolation does not regularly identify suspicious activity, as transactions may not appear unusual or suspicious on their own. It is important to consider TM alerts alongside KYC information, proactive intelligence-led analysis, hidden or linked relationships, changes in UBOs (ultimate beneficial owner) and other relevant information to help identify suspicious activity.

11.5 Most firms appear to find it easier to identify instances of market abuse than ML. Some firms are combatting this through closer working and collaboration between TS and TM teams. However, this area still requires significant consideration by firms. We noted that larger firms had separate TS and TM teams, whereas smaller firms often used the same personnel. This topic was also highlighted in TR19/4 and closer consideration of market abuse and financial crime is encouraged in the FCA's Financial Crime Guide 8.1.10. Firms have found that SARs often originate from TS alerts and STORs, and through applying a ML lens and using KYC data led to suspicions of ML being identified. Firms must consider their obligations in relation to financial crime when they have identified activity they suspect may amount to market manipulation and/or insider trading, and should the customer seek to use or transfer the proceeds relating to the suspicious activity.

Figure 11: Shows the variety of TS and TM alerts we saw at firms and how teams are collaborating - to demonstrate good practice and help firms in considering ways to enhance their systems and controls.

Trade Surveillance (TS)

Aim: Detect and prevent market abuse to preserve market integrity. Suspicious transaction and order reports (STORs) are raised to us.

Examples of firm alerts seen include:

- trading on illiquid or low-volume securities
- free of payment
- back-to-back trading (wash / circular / cross)
- broker order to trade ratio
- excessive cancels
- ramping
- spoofing/layering
- trade price to close price and marking the close
- abnormal trade
- front running trade monitoring within specified time frame (insider dealing)

Transaction Monitoring (TM)

Aim: Identify unusual activity that could constitute suspicions of ML. Suspicious activity reports (SARs) are raised to the UKFIU (NCA).

Examples of firm alerts seen include:

- split transactions
- transactions from one to many or vice versa
- client receives/sends and back almost same amount in same day
- multiple money movements across borders/high risk jurisdictions
- FATF plenary and grey list
- multiple transactions or cumulative amounts in period
- fund more than expectations or SoW
- spikes in activity for high-risk client
- trade size and frequency anomalies, suspicious counterparties, immediate trading in size on account opening, changing client behaviour (products/size of transactions)
- unusual trading patterns
- uneconomic or irrational trading
- third-party payments
- geographical destination or origin of transaction
- payments/receipts with no link to business
- bank transfer instructions with equal amounts in/out

Examples of TS and TM collaboration

- integrated teams
- collective MI reporting
- sharing alerts for read-across
- sharing information, themes, lessons learned, intelligence
- joint training
- shared reporting lines
- regular meetings and collaboration calls
- collective risk assessments
- working on client remediation together
- clear communication and escalation channels
- involving Relationship Managers, front and middle office, compliance

Integrated process where TM/TS alerts are considered in KYC/CDD, CRA, BWRA, training, MI reporting, policies and procedures – to ensure effective systems, controls and identification of suspicious activity.

11.6 We noted limited instances where TM has been used as part of an integrated process to help with ongoing monitoring, risk assessment, KYC and record keeping processes. Firms should make sure TM alerts are appropriately considered and integrated into financial crime controls to mitigate MLTM risk more robustly.

11.7 Equally, many firms did not appear to have considered how best to use KYC and customer information to support, refine and make TM more effective. Some firms incorporate customers' expected behaviour into alert management systems. However, many firms do not consider customer risk ratings, customer activity, jurisdiction risk, customer information or business/market risk when configuring and maintaining TS and TM alert and control frameworks. Historical transactions are not often reviewed when new adverse media or information from ongoing monitoring arises.

11.8 Firms have generally found that more financial crime suspicions are escalated from the front office who see the activity as it happens. Firms should continue to provide further support and training to make sure that front and middle office have greater responsibility for and ability to identify and raise suspicions.

11.9 While the lack of visibility of the whole transaction chain is a constraint to identifying potential ML activity, firms should consider whether to raise SARs when there are appropriate suspicions, even if only part of the transaction is visible.

11.10 Many firms are considering how best to use technology to help with TM. However, none of the firms we observed had made significant progress in understanding how AI (artificial intelligence) could be used for both TM and onboarding processes. For wider awareness, an AI and machine learning survey has been undertaken separately to this MLTM work, to understand the use of AI in UK financial services and its implications.

11.11 The following TM related case studies are for firm awareness and consideration.

Case Study 20

The firm's front office raised their suspicions, where a non-UK client placed an aggressive price limit order compared to market expectations. The broker flagged this to compliance.

A subsequent KYC review found the client was a broking arm of a wealthy overseas family office and had only traded one security before. The trade was stopped and the client exited.

Case Study 21

The firm uses third-party software to generate TS and TM alerts. These alerts are configured with the provider and reviewed for appropriateness on a periodic basis. The alerts are also configured per client and product.

A daily joint team review is undertaken of the alerts received, transactions made and any rationale for discounting or progressing each alert.

The level of false positives received from the software is reviewed, considered and accepted to manage risk.

Our expectations of firms

11.12 Firms need to complete appropriate TM to make sure that transactions are consistent with the firm's knowledge of the customer, the customer's business and risk profile. A variety of approaches are required to enhance and maximise TM as part of an effective financial crime framework. Front office contributions, cross-functional investigations, TS and TM systems, and KYC staff should work collaboratively to ensure MLTM risk is managed and mitigated appropriately.

Good practices identified

- Embedding risk typologies into TM and TS procedures.
- Regularly reviewing the TM system configuration to make sure it remains appropriate and effective at managing the risks.
- The rationale for discounting TM alerts is clearly documented.
- TM rules are customised for particular clients and product activity.
- ML suspicions are considered when reviewing TS alerts.
- The number of false alerts, resourcing required, and residual risk are considered when determining TM controls and system configuration.
- TS and TM teams work closely, share information, provide cross training, joint reporting, joint risk recording, share high-risk clients lists and accounts of focus, and having clear escalation routes.
- Compiling a view of actual customer activity over time – comparing this to the KYC information held, discussing it with the customer and updating records where appropriate.
- Considering actual trade activity against KYC information and triggering a review of the account where appropriate.
- Inclusion of AML 'risk words' in communication surveillance tools and controls.
- Documenting the risks faced and mitigating TS/TM controls.
- Considering whether POCA (Proceeds of Crime Act 2002) requires the submission of a SAR where a STOR is raised.
- Completing an event-driven review of a customer's KYC following notification from an exchange of a transaction they are investigating.

Poor practices identified

- Attitudes that market knowledge and experience alone will enable effective identification of suspicious activity.
- TS and TM alerts are not considered in KYC CDD processes, reviews and recorded on customer files as part of a cyclical process.
- Unscalable manual solutions given the level of firm resourcing and business growth.
- Insufficient risk-based justification for not completing TM for all types of business.
- No documented record of reviews completed on transactions or alerts.
- Only considering the risk of ML from a TS alert if a STOR is raised.
- TS/TM controls mostly focusing on identifying market abuse.
- Minimal guidance and support given to front and middle office to help them to identify and report suspicious activity.
- Front and middle office are not working together to identify suspicious activity.
- TM alert activity and themes are not fed back into controls, training and risk assessments.
- Insufficient resources to manage financial crime effectively and limited financial crime knowledge and experience throughout the business.

Part 2: Findings

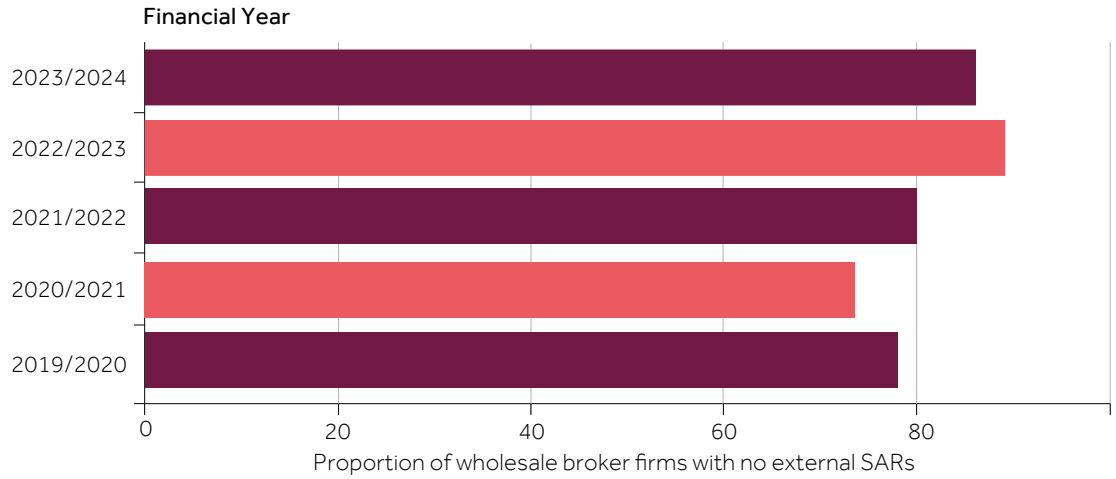
Chapter 12

Investigations and suspicious activity reporting (SAR)

What this is

12.1 Regulation 28(11)(a) of the MLRs requires firms to undertake scrutiny of transactions undertaken throughout the course of the relationship. Firms are required to comply with the MLRs, POCA, and the TACT (Terrorism Act 2000) to investigate and disclose any suspicious activity.

Figure 12: Proportion of all wholesale brokers that have disclosed no SARs to the NCA (National Crime Agency) over the last 5 years (REP-CRIM data as of 1 October 2024)



12.2 As of 1 October 2024, REP-CRIM 2023/24 submissions suggest that nearly 75% of wholesale broker firms reported that they have not refused or exited any customers and have also not disclosed any SARs to the NCA during the period.

12.3 Firm SAR submissions that we saw and UKFIU guidance indicate that good quality SARs have the following characteristics:

- They explain why the activity is suspicious, not in line with expectations, and provide a clear and specific rationale to support a suspicion of ML.
- Firm analysis is completed first to provide useful information in the SAR.
- Details of investigation carried out are documented on the case, including details of any STOR references and how the risk has been mitigated.
- Include pertinent account(s) details, KYC information and intelligence gathered to support case and enable law enforcement to make wider enquiries.
- Identify and explain specific red flags and why the activity is deemed to be suspicious.

- Include details of pertinent transactions, amounts, dates, times, products and what was traded (including full name and ISIN (international securities identification number)), to illustrate the activity leading to the suspicion.
- Use simple language, avoiding acronyms or technical jargon, so that it can be understood by anyone less familiar with the scenario or processes.
- Provide context, for example, what part of the transaction chain can or cannot be seen.
- Multiple SAR glossary codes used where suspicion covers several topics.
- Briefly summarise the issue and articulate themes and patterns of behaviour, rather than simply listing previous SARs submitted.
- Include details of the risk or name the identified typology.
- Explain how any cited open-source information support the suspicion.

What we saw

12.4 Our review of firms' SAR procedures and selected SARs submitted noted that:

- Wholesale brokers have limited knowledge and experience of using the MLTM glossary code and rarely reference the code in SAR policies and procedures. Engagement with industry, however, taught us that other market participants such as wholesale banks are more familiar and comfortable with the MLTM glossary code and are actively using it.
- There are low numbers of external SARs submitted by wholesale brokers - this is echoed in REP-CRIM returns – see Figure 12. While not necessarily indicative of an issue, firms should satisfy themselves that their processes are operating effectively.
- The MLTM SARs glossary code was not consistently used in line with UKFIU guidance.
- We noted instances where wholesale brokers believe they are unlikely to identify any suspicious activity and submit SARs on the basis that they only see one side of the trade and believe their business and clients are low risk.
- Several firms consider and document the rationale for raising a SAR when submitting a STOR (see our previous industry letter on the topic to help with this).
- The standard of investigations completed, and quality of SARs documented requires improvement.
- Type and number of SARs raised rarely feeds into a customer's KYC, CRA rating and ongoing monitoring.
- STORs (for example, suspicions on a counterparty) are sometimes passed to AML teams for assessment considering KYC information they hold.

12.5 We saw instances where firms incorrectly used the MLTM glossary code to report suspicions of market abuse. We also saw cases where the MLTM glossary code wasn't used, despite there being suspicions resulting from the seller's secretive nature, company structure, illogical transaction details, understanding of the instrument and market, as well as other red flags. Incorrectly using SAR glossary codes affects the collection, collation and analysis of suspicions. This could delay or constrain investigations, as well as the assessment and monitoring of holistic risks over time, in support of the strategic response to MLTM.

12.6 Firms do not appear yet to have understood or considered how they can use the recently enacted ECCTA information sharing measures and guidance to counter money laundering, raise awareness and intelligence and reduce MLTM risk. We found very little sharing of information between wholesale brokers and across the market. Few wholesale broker firms participate in and are represented in market forums and working groups.

Our expectations of firms

12.7 Where suspicions arise firms should investigate, document and disclose any suspicions appropriately.

Good practices identified

- SAR reports that include pertinent details, triggers, and rationale for suspicions.
- Using internal KYC information and external research to support investigation of suspicious activity.
- Documenting a rationale where a SAR was/was not submitted to the NCA and considering the effectiveness of controls in identifying suspicious activity.
- Reviewing a customer's previous activity to understand the firm risk and impact when suspicious activity is identified.
- Submitting SARs where the firm knows or suspects an entity is engaged in money laundering, dealing in criminal property, or suspects that proceeds of crime are passing through market trades.
- STOR read-across to highlight ML suspicions – considering dual reporting of SAR/STOR where appropriate.
- Triggering ad hoc reviews of customers where a SAR has been raised, to re-assess the risk posed by the customer.
- Reviewing SARs raised to evaluate the risk posed to the firm and its controls.
- Comparing historic SAR patterns and themes, especially where the customer is the same or linked to previous SAR reporting submissions.
- Submitting a SAR following a police investigation on a previous customer they were informed about.
- Whistleblowing policies and awareness initiatives at firms which encourage disclosures that could lead to wider MLTM suspicions and intelligence.

Poor practices identified

- Details of SAR analysis and outcomes are insufficiently documented.
- SARs raised are not considered in KYC, customer risk ratings and staff training.
- Policies and procedures do not include the MLTM SAR glossary code, there is low awareness of the code, and the code is often used inappropriately.
- Lack of participation in industry forums and sharing of information.

Part 2: Findings

Chapter 13

Training, resourcing and policies and procedures

What this is

13.1 Firms are responsible for making sure that financial crime systems and controls are supported by appropriate resourcing, training and formal policies and procedures in line with Regulation 19 and 24 of the MLRs. Further support is in paragraphs 2.2.5-6 of the FCA Financial Crime Guide.

What we saw

13.2 Training is vital to raise awareness of financial crime risk and support systems and controls. We found most firms have annual financial crime training, often using external providers that offer computer-based courses, training materials and track the completion of training.

13.3 Proactive firms tailored training content to their business model, related risks, common red flags and for the different roles in the firm. Some also delivered face-to-face training. One firm invited external speakers to provide training, and others provided specific in-house training to front office and business support functions. Larger firms often provide compliance advisory support to front office staff. This gives them additional guidance to help identify, understand and report suspicions, since they are likely involved in customer transactions. However, amendments to policies and procedures are rarely formally acknowledged by staff or included in annual training to make sure they have been read and understood.

13.4 Resourcing in AML or financial crime functions varies greatly across firms and some firms appear to be under-resourced for their number of customers. This could have a direct impact on the quality and timely completion of onboarding and periodic reviews for example. We also noted that resourcing has often not increased in line with business growth. Some smaller firms have trained wider teams in AML processes so they can support onboarding or review activities and provide the firm with more flexible resourcing.

13.5 It is imperative that processes are formally documented, and knowledge shared among teams, particularly where a firm is small, and the loss of personnel would be disruptive. Several firms relied on the belief that extensive industry and trading experience will naturally enable staff to spot suspicions, without considering the risks and implications of this informal approach.

Our expectations of firms

13.6 Firms must have appropriate levels of resourcing to support the effective operation of its systems and controls. Staff should receive training that is suitable to the role performed and risks the business is exposed to. Firms must also have up-to-date policies and procedures appropriate to its business.

Good practices identified

- Enhancing generic training with business and role specific content.
- Cross training TM, TS, AML, front office teams on relevant risks, typologies and case studies.
- Using 'near misses' data (for example, where QA/QC has highlighted processes not being followed correctly) to identify and deliver additional training.
- Testing effectiveness of training, for example, alerts raised, spot checks, feedback.
- Periodic reviews, approval, rollout and tracking of policies and procedures.
- Additional red flag training to remind staff of their obligations, in response to a reduction in internal SARs raised over the year.
- Financial crime training delivered to non-executive directors.
- Disseminating key points from 'Dear CEO (Chief Executive Officer) letters', final notices, regulatory changes, and useful articles in cascades to all staff.

Poor practices identified

- Insufficient resourcing given number of customers and business growth.
- Relying on individuals' experience and knowledge instead of documenting policies and procedures.
- Training not being completed on time, nor escalated to management for action.

Part 3: Next steps

Chapter 14

Next steps

14.1 We need a collaborative effort to reduce the risk of MLTM and to:

- Raise awareness of MLTM.
- Increase the identification and reporting of suspicions.
- Improve the sharing, discussion and review of MLTM information, typologies and best practice.
- Implement robust systems and controls.
- Deter and reduce the risk of MLTM in the future.

Firms next steps

Firms need to continue to review their systems, controls, and MLTM awareness and training to ensure they meet the required standards and are effective in the fight against financial crime. In particular:

- ☑ Firms should consider and appropriately document the MLTM risk posed to and by the firm, ensuring it is reflected in their BWRA and systems and controls.
- ☑ Firms should consider how best to use TM as part of an integrated process of financial crime systems and controls, incorporating tailored TM controls and alerts. Further collaboration between TM, TS, front and middle office teams should be encouraged and facilitated by firms.
- ☑ Firms should ensure they have firm and role specific MLTM staff training and awareness in place.
- ☑ Firms should ensure their relevant teams are aware of the UKFIU MLTM SARs glossary code, are using it appropriately, and are submitting quality SAR reporting.
- ☑ Firms should also review the recently enacted ECCTA and consider how they can share information to counter money laundering, raise awareness and intelligence and reduce MLTM risk.

Our next steps

We will:

- Make sure that firms assessed as part of this MLTM review, and those reviewed in the future, take steps to consider this report, identify and implement change where needed. We will continually prompt improvements to reduce risk across the markets.
- Work closely with industry and partners to understand typologies and share information and intelligence as appropriate about emerging risks, issues and best practice to collectively increase disruption opportunities and reduce the risk of MLTM.
- Work with firms and other stakeholders to establish if existing FCA held datasets can be used to proactively identify MLTM and enable further proactive supervision.
- Encourage greater innovation by firms and third-party providers so that TM systems and alerts become more tailored to capital markets and more effective in identifying potential MLTM.
- Work with the UKFIU to ensure better use of the MLTM SARs glossary code to raise awareness of suspicions. Encouraging the improvement of high-quality SAR reporting will also help with these efforts.

Annex 1

Abbreviations used

Abbreviation	Description
ABC	Anti Bribery and Corruption
AML	Anti-Money Laundering
AI	Artificial Intelligence
BWRA	Business-Wide Risk Assessment
CASS	Client Asset Sourcebook
CDD	Customer Due Diligence
CEO	Chief Executive Officer
CIO	Chief Information Officer
COO	Chief Operating Officer
CRA	Customer Risk Assessment
DAML	Defence Against Money Laundering
ECCTA	Economic Crime and Corporate Transparency Act 2023
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FC	Financial Crime
FI	Financial Institution
FoP	Free of Payment
IDB	Inter-Dealer Broker
ID&V	Identity & Verification
IMEI	International Mobile Equipment Identity

Abbreviation	Description
ISIN	International Securities Identification Number
JMLSG	Joint Money Laundering Steering Group
KYC	Know Your Customer
LE	Law Enforcement
MAC	Media Access Controls
MI	Management Information
ML	Money Laundering
MLR	Money Laundering Regulations 2017
MLRO	Money Laundering Reporting Officer
MLTM	Money Laundering Through the Markets
MTF	Multilateral Trading Facility
NCA	National Crime Agency
OTF	Organised Trading Facility
PEP	Politically Exposed Person
PF	Proliferation Finance
POCA	Proceeds of Crime Act 2002
QA	Quality Assurance
QC	Quality Control
SAR	Suspicious Activity Reporting
SDD	Simplified Due Diligence
SMF	Senior Management Function
SoF	Source of Funds
SoW	Source of Wealth
STOR	Suspicious Transaction and Order Reports

Abbreviation	Description
TACT	Terrorism Act 2000
TCSP	Trust or Company Service Providers
TF	Terrorist Financing
TM	Transaction Monitoring
TS	Trade Surveillance
UBO	Ultimate Beneficial Owner
UKFIU	UK Financial Intelligence Unit

Pub ref: 1-008395

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