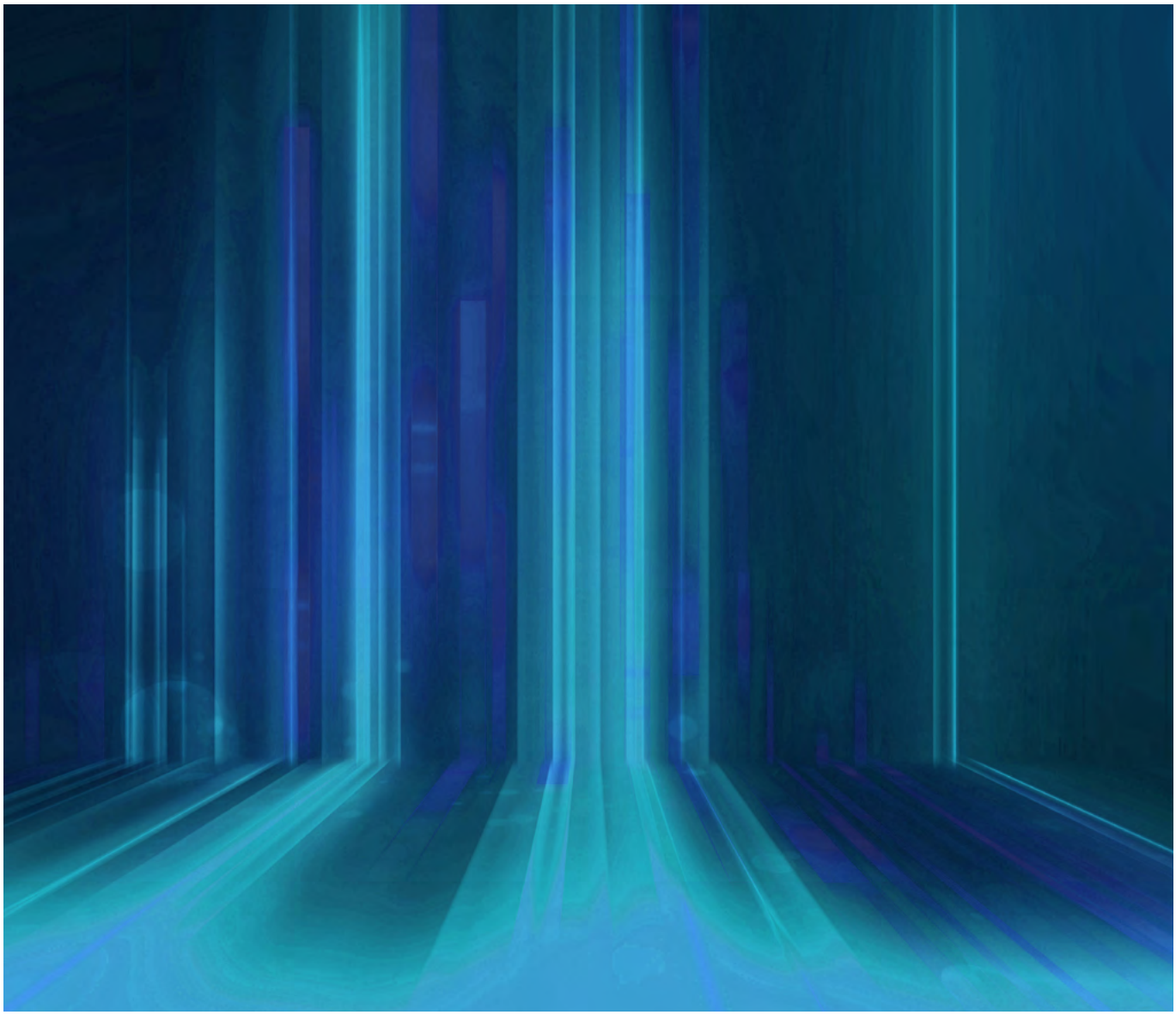
afme/
Finance for Europe

EY
Building a better working world

Anti-Money Laundering Transaction Monitoring in the Markets Sector

An industry perspective

October 2021



Association for Financial Markets in Europe
www.afme.eu

Disclaimer

The Anti-Money Laundering Transaction Monitoring in the Markets sector report (the "Report") is intended for general information only and is not intended to be and should not be relied upon as being legal, financial, investment, tax, regulatory business, or other professional advice. AFME doesn't represent or warrant that the Report is accurate, suitable, or complete and none of AFME, or its respective employees shall have any liability arising from, or relating to, the use of this Report or its contents.

Your receipt of this document is subject to paragraphs 3, 4, 5, 9, 10, 11 and 13 of the Terms of Use which are applicable to AFME's website (available at http://www.afme.eu/en/about-us/terms-conditions) and, for the purposes of such Terms of Use, this document shall be considered a "Material" (regardless of whether you have received or accessed it via AFME's website or otherwise).

October 2021

Contents

Foreword

AFME is pleased to publish "Anti-Money Laundering Transaction Monitoring in the Markets sector" in collaboration with EY.

A key challenge that the industry faces is how to best identify money laundering activities. This has intensified in recent years following high profile cases in the capital markets space which has, understandably increased regulatory scrutiny of firms' Anti-Money Laundering (AML) controls.

Firms do already have established Anti-Financial Crime programmes, designed to detect suspicion of money laundering, supported by AML transaction monitoring (TM). In this paper we consider the effectiveness of the processes that make up a firms AML TM control framework and provide a road map to support firms in designing and operating the most effective solution.

To enable this, we have explored several key themes in the preparation of this paper. We consider how effective the current AML TM approaches in the markets sector are and we review the results that they yield. We identify how existing AML TM systems can be enhanced and we consider the evolving skillset that is needed to support this. We also look at the use of data, technology, and enhanced analytics to further drive improvements, building stronger more efficient solutions and leveraging opportunities for intelligence-led investigations. We also review the processes around the submission of Suspicious Activity Reports (SARs) and explore the advantages to the sector as a whole in establishing greater collaboration between private and public sector bodies. We conclude by considering the benefits of convergence, between market abuse surveillance function and the AML TM function.

AFME represents European wholesale firms' and this paper is specifically targeted at its Members. Whilst this paper is not intended to be an exhaustive list of required changes and the key points covered in this paper may not apply to all firms, we expect much of what follows will be relevant across the industry. In planning and executing their Anti Money Laundering Transaction Monitoring strategy Global firms will of course have to consider differences in local law and regulation, as well as the specifics of their unique business model.

AFME would like to thank EY for their support in the production of this report, as well as Members from AFME's Financial Crime Working Group and Compliance Committee, all of whom made contributions that were integral to the development of this publication. We are grateful to all those who have participated in this paper, including Member firms, European regulators, law enforcement agencies and financial intelligence units (FIUs).

This joins a series of papers produced by AFME and EY including Governance of Market Abuse Surveillance[1] Controls, The Future of the Compliance Control Environment[2] and The Scope and Evolution of Compliance[3].

James Kemp
Managing Director
GFMA and AFME

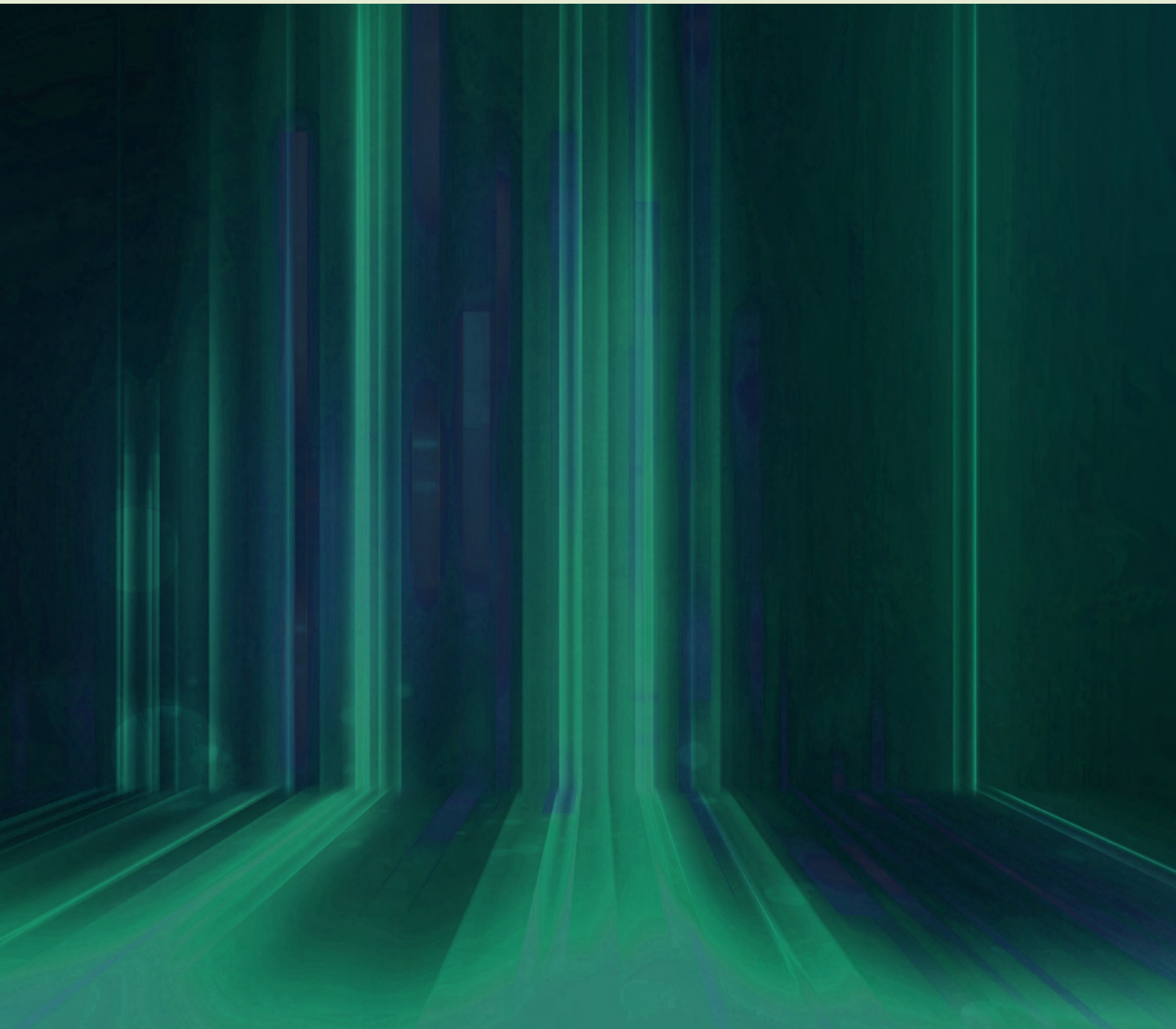
1 www.afme.eu/Portals/0/DispatchFeaturedImages/AFME%20Market%20Abuse%20Surveillance%20Governance-An%20industry%20perspective_FINAL%20(1).pdf

2 https://www.afme.eu/Portals/0/DispatchFeaturedImages/The%20Future%20of%20the%20Compliance%20Control%20Environment-FINAL.pdf

3 https://www.afme.eu/Portals/0/DispatchFeaturedImages/AFME_FutureCompliance_FINAL-1.pdf

Anti-Money Laundering Transaction Monitoring in the Markets Sector

An industry perspective



Introduction

In response to interest from AFME (the Association of Financial Markets in Europe) Members, AFME engaged EY to conduct a study into current practices and the future direction of Anti Money Laundering (AML) transaction monitoring (TM) in the markets sector. The resulting paper is based on:

- In depth interviews with AFME Members;
- In depth interviews with European regulators, law enforcement agencies and financial intelligence units (FIUs);
- Survey responses from Member banks; and
- Additional insights from AFME and EY.

In the private sector, the interviews and survey focussed on activities in the European region, however the respondents were a combination of European headquartered banks (France, Germany, Italy, UK and the Nordic region) and leading US, Canadian and Japanese banks with operations in Europe. Respondents' activities covered all asset classes including issuance and trading of financial instruments in equities, fixed income, foreign exchange, commodities and money markets.

The survey respondents self-assessed with a range of maturity levels from Immature to Leading (Figure)[4]

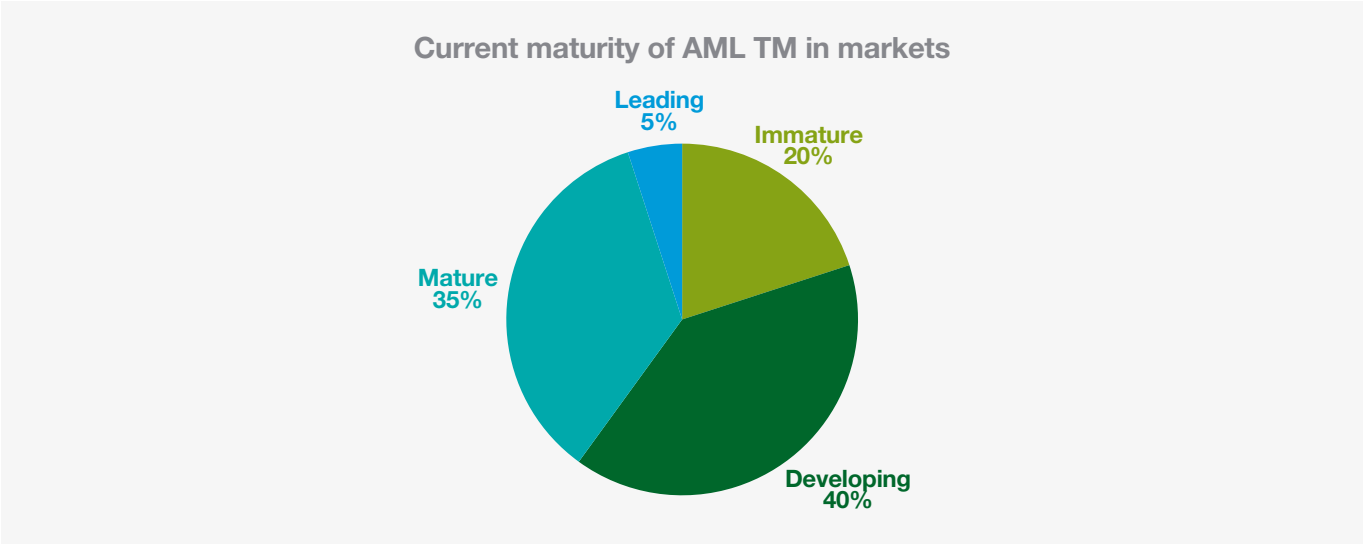


Figure 1: **Firms self-assessed maturity of control for AML TM in Markets**

Respondents on the public sector side included regulators, law enforcement agencies and financial intelligence units from several European countries.

The analysis was conducted between June and September 2021.

4 The maturity level definitions are:
1. Immature: basic monitoring undertaken with gaps
2. Developing: good coverage using basic processes
3. Mature: well-developed processes that have evolved and provide the business with a rich set of surveillance controls
4. Leading: consistent focus and investment in innovation of techniques and processes to improve surveillance controls above and beyond the existing comprehensive coverage

Executive Summary

A key part of any Anti-Financial Crime programme is the ongoing monitoring of financial transactions for suspicion of money laundering, known as anti-money laundering (AML) transaction monitoring (TM). This has been a regulatory requirement for all financial services firms across Europe for the past 20 years. In that time, a wide range of vendor software products have evolved that work effectively, if not always efficiently, for retail and business banking. But those same systems have also demonstrated limited effectiveness in the markets[5], sector when implemented on a standalone basis. This is due to a number of factors; 1. the significant market-driven volumes of rapidly executed high-value transactions creating a challenge in identifying something unusual and 2. the lack of visibility that firms may have over clients and their activity.

Regulatory attention in this area continues to increase. In the past six years, two CEOs of major European banks have resigned due to, or in part due to, issues with AML controls in their markets' activities.

This paper is based on survey results and interviews with banking firms, regulators, law enforcement agencies and financial intelligence units across Europe. It sets out the current state of play of AML TM in the markets sector in the European region, proposes how to perform more effective monitoring, and identifies several emerging themes for the future.

The key themes are:

1

Current AML TM systems are ineffective in the markets sector…

- 80% of firms surveyed filed zero Suspicious Activity Reports (SARs) for their markets business from alerts generated by AML TM systems in the past year;
- 95% of SARs filings in this sector originate from market abuse cases (as predicate offences) or front office referrals;
- There is a widely held view amongst the private sector that money laundering is likely to be going undetected.

2

A small number of firms have demonstrated that it is possible to monitor effectively through the use of a hybrid approach blending technology tooling and automated techniques with highly skilled manual processes …

- A small number of banks are successfully identifying suspicious activity and reporting it;
- Traditional AML TM systems can yield meaningful alerts when enhanced with additional data and more sophisticated detection that leverages machine learning and network analytics;
- Firms using a hybrid approach are deploying more markets-specific AML TM coupled with intelligence-led investigations;
- It is essential to complement automated AML TM systems with proactive, intelligence-led analysis to support effective outcomes.

3

The key to deploying analytical TM solutions successfully in the markets sector is using highly skilled team members that understand the complex domain as well as the technical methods…

- To perform more effective monitoring requires senior management support and investment in technology;
- It also requires highly skilled analysts;
- Manual referrals and front office perspective will continue to be a key pillar in intelligence gathering;
- Another important element is the ability to legally and openly share data between financial institutions, particularly to help identify end counterparties when there are brokers or central counterparties and when money laundering risks or suspicions exist;
- Ultimately, monitoring performed with the aid of shared utility services may be a more effective solution, but would require a coordinated resolution of a number of inhibitors and therefore is currently unlikely to happen in the short term.

5 By "markets" we mean the primary issuance and secondary trading of financial instruments in equities, fixed income, commodities, credit, foreign exchange, real estate and similar asset classes. This does not include transaction banking products such as correspondent banking or trade finance.

4

More collaboration between private and public sector would be beneficial …

- There is very little feedback on SARs submitted so firms do not often know if a SAR has led to a positive investigation for money laundering and do not have reliable feedback to assess effectiveness of different tools and techniques;
- Whilst there is good general AML guidance from regulators, there is little specific threat or intelligence-based guidance from the public sector;
- It is not feasible for law enforcement agencies to give feedback on individual SARs. However, more collaboration between the industry, regulators, law enforcement and FIUs would be beneficial to all.

5

Greater effectiveness and cost efficiencies will be achieved through partial convergence of market abuse surveillance with AML TM…

- There is a trend towards operational convergence of market abuse surveillance and AML TM, particularly with respect to overall management and governance of these functions;
- There is an opportunity to leverage data and technology investments in market abuse surveillance for AML TM;
- However, full technology convergence between the two functions is unlikely due to differences in timeframes, data, typologies, etc.

A force for change…

In conclusion, although current AML TM systems are widely considered to offer limited effectiveness in the markets sector, there is much more that can – and should – be done to identify money laundering that may be falling beneath the radar.

Current state – AML TM is ineffective in the Markets Sector

SARs statistics

In the retail and business banking sectors, most Suspicious Activity Reports (SARs) originate from alerts generated by AML TM systems, with additional SARs resulting from manual referrals from bank staff. In the markets sector, 80% of the firms in our survey filed zero SARs from AML TM alerts in the past year, some of them major global banks spending millions of Euros per year on AML TM systems and operations. Of those who did file SARs from AML TM alerts, the volumes were low compared to SARs originating elsewhere. Annual SARs volumes published by the UK's National Crime Authority[6] show only 150 SARs for 2019/20 attributed to capital markets, representing less than 0.1% of all SARs (573,085).

By comparison, in retail and business banking, conversion rates from AML TM alerts to SARs are typically in the 10-20% range[7].

The best sources of SARs filings in the markets sector are referrals from market abuse investigations and referrals from front office staff, for instance desk supervisors who spot something suspicious (Figure). In most cases, firms already have robust processes in place whereby Suspicious Transaction and Order Reports (STORs)[8], indicating possible market abuse, are automatically referred to the AML team for additional investigation. Less common is the other way around, where cases originating in the AML space are referred to the market abuse team, but one bank in our survey did cite this as a practice they had implemented and found to be productive.

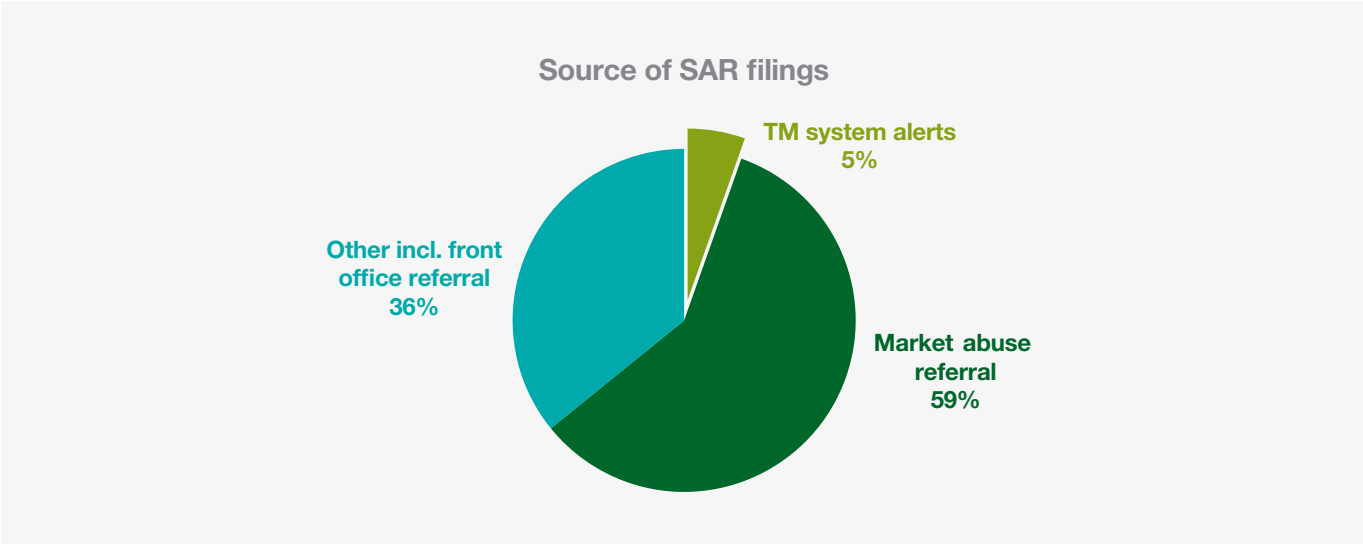


Figure 2: **Originating source for information resulting in a SAR filing**

6 UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2020, National Crime Agency

7 EY EMEIA AML Transaction Monitoring Survey 2018

8 See Appendix A for an overview of STORs and SARs

Is money laundering going undetected?

There is a generally held belief that money laundering may be going undetected, though opinion is divided as to how significant this is (Figure).

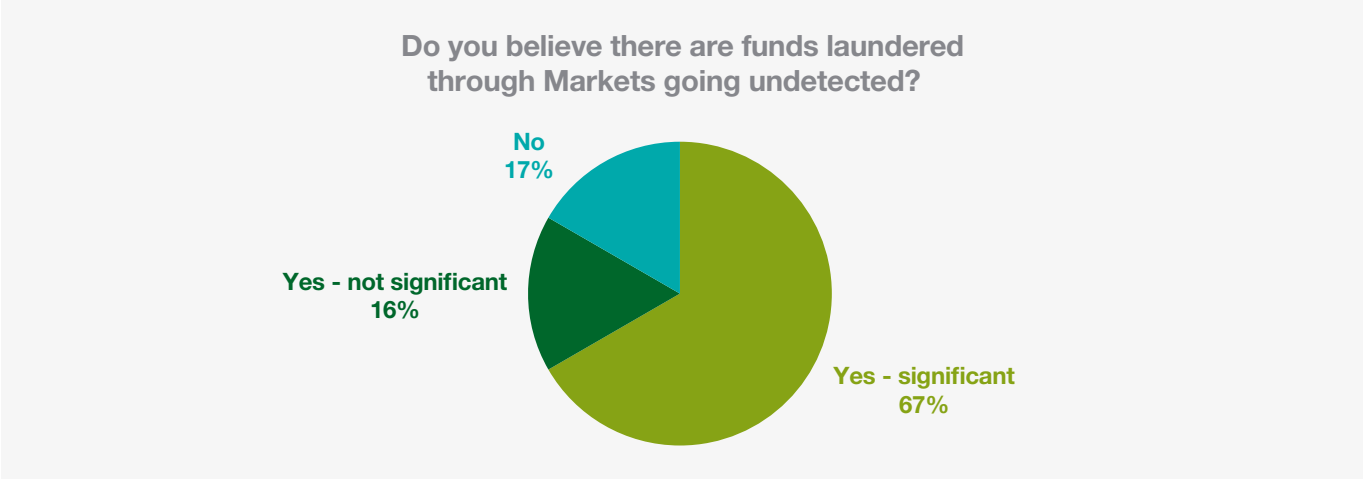


Figure 3: **The extent to which interviewees believe money laundering may be going undetected**

Mostly this is supposition based on the idea that the high value and often cross-border nature of trading is attractive to money launderers, and some firms gave additional rationale for stating that they believe the value of undetected nefarious activity to be significant. In some cases, firms had observed and reported suspicious activity but did not have sufficient information available to identify the ultimate beneficiaries. Some firms also cited the fact that intelligence-led investigations often revealed suspicious activity worthy of a SAR filing that the automated TM system had failed to detect. One organisation using a more advanced 'hybrid approach' (see section 4) is now identifying tens of SARs per year (in addition to STOR initiated SARs) and has uncovered concerning cases involving significant amounts of suspicious activity akin to wash trading.

Several organisations (including regulators and law enforcement) made the obvious point that, almost by definition, we simply don't know what is out there that is undetected. What does seem reasonable to determine is that money laundering in this sector is likely to be relatively low in volume compared to the retail sector but, when it does occur, is very high in value.

"There is a collectively-held recognition across law enforcement, regulators and reporters that there are significant intelligence gaps relating to the scale of illicit finance generated in the UK and overseas but whose MLTM (Money laundering through markets) impacts the UK specifically."

UK National Crime Agency, May 2021[9]

Current state of transaction monitoring

Focussing specifically on AML TM for markets, currently firms use a number of detection methods (Figure) with a variety of detection typologies implemented. The majority of firms have some form of automated AML TM in place and also take referrals from the market abuse surveillance team. Some firms will also run periodic reports to identify anomalous behaviour and in some cases financial crime teams will receive referrals from front office or operations team members. Whilst these referrals received are lower in volume, they tend to result in SARs more often. These cases reiterate the importance of good, regular financial crime training across the enterprise.

9 https://www.nationalcrimeagency.gov.uk/who-we-are/publications/517-glossary-codes-and-reporting-routes-may-2021/file

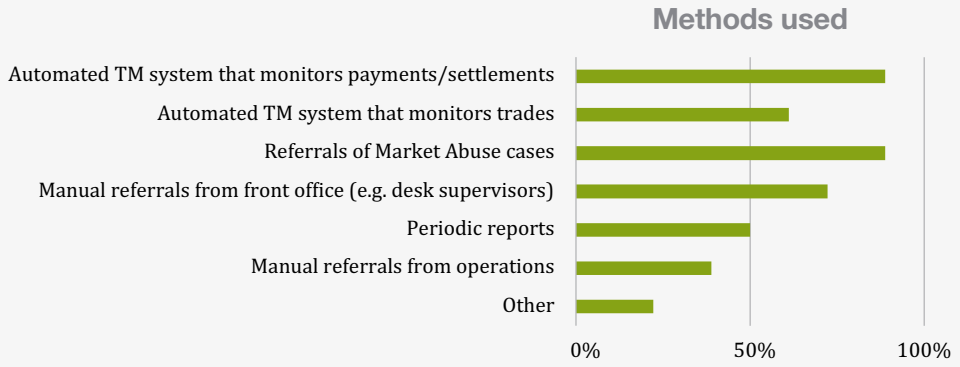


Figure 4: **Markets AML TM methods used**

In retail and business banking there are a number of "classic" typologies that are well-established as the standard AML TM typologies, for example rapid movement of funds or changes in behaviour. Many firms report these to be the typologies that have been applied across markets products too with little consideration for their applicability to this very different domain.

However, over recent years more and more firms have begun to implement "markets-specific" typologies aimed at known risk types for markets products. Mirror trading and wash trading are currently the most prevalent of these[10] (see Figure). It is important to note that most of both the classic typologies and the markets-specific typologies are, in general, not considered to be very effective.

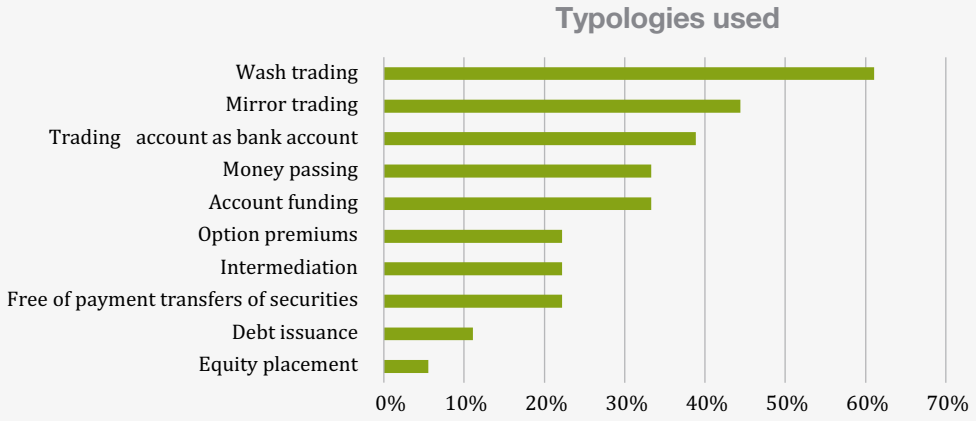


Figure 5: **Markets-specific AML TM typologies used by firms**

10 See Appendix B for definitions of these typologies

Operating model

In terms of the operating model there is no standard as to where AML TM sits (Figure) or who has responsibility for it (Figure), but the investigation process is fairly standardised, with the majority of banks operating a three level investigation process followed by a SAR filing step, and a few banks just having a two level process (in addition to SAR filing).

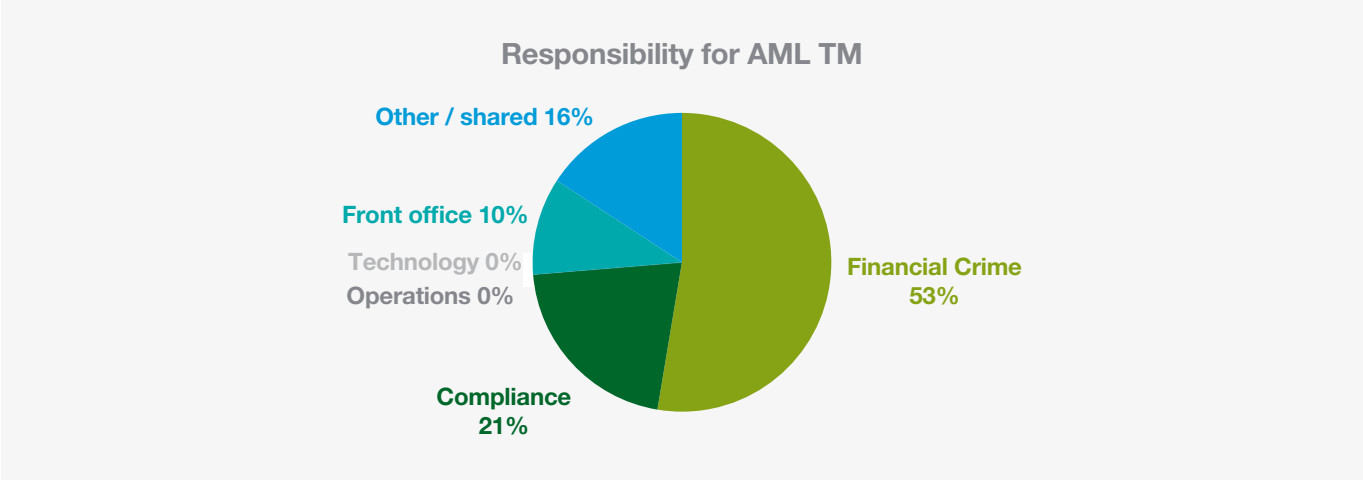


Figure 6: **Team responsible for AML TM**

The majority (53%) of firms have a dedicated 'Financial Crime' team that will hold responsibility for AML alert investigation, alongside other anti-financial crime activities, such as customer due diligence and sanctions screening.

The key decision over which team of analysts is responsible for reviewing, investigating and disposing of alerts is one based on primarily skillset (and where this naturally sits within the business) as well as operational feasibility. The two teams typically used are the broader financial crime or AML investigations team, who for the large group of banks with a retail/business bank will be the team that handle the AML alerts from this part of the bank, and then the market abuse investigations team, who tend to have smaller teams with less financial crime experience but much greater insight into markets products and processes.

Investigations undertaken by broader retail/business AML alert review team	Investigations within market abuse surveillance team
• Use of well-established processes with supporting technology in place and teams operationally experienced in the disposition procedures • Typically, a larger team able to scale and handle greater variations in alert volumes • Sometimes use near-shore or off-shore resources, particularly for level 1 filtering, to give greater efficiencies • Good financial crime knowledge and experience in team members but typically less experience and knowledge in markets' products and markets' specific typologies. • Ability to assess broad client risk across markets and non-markets (retail/business) products	• Team members with strong understanding of markets' products, clients and market dynamics • Sometimes individuals are aligned to individual asset classes to provide even greater depth of market understanding • Existing close relationships with Front Office to query as needed • Typically, smaller teams with market abuse responsibilities too can cause bandwidth constraints • Team members have strong background in market abuse but less experience in anti-money laundering and terrorist financing

Some firms have developed a hybrid model where the broader bank's AML alert review team may perform level 1 review of markets alerts, sometimes using offshore/nearshore resources, whilst a smaller markets specific Financial Crime team or the market abuse team may then investigate the cases that have been escalated to level 2 or level 3 investigation.

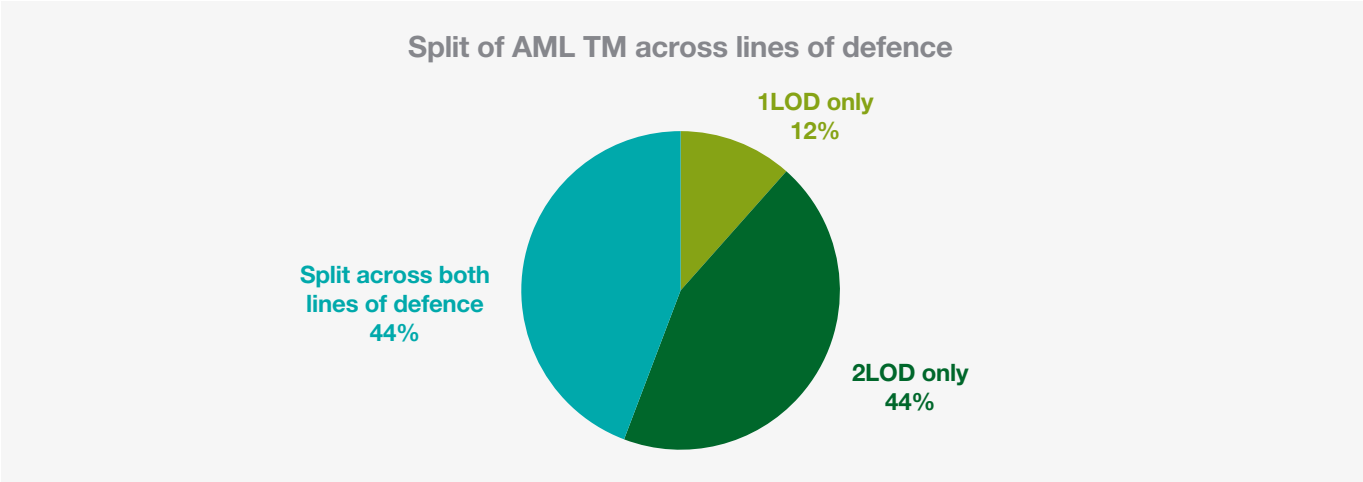


Figure 7: **Responsibility for AML TM across the lines of defence**

Effective TM requires a hybrid approach

Drivers for change and investments in new technology

Most firms we spoke to are undergoing transformation programmes for their markets AML TM. This is partly due to increasing interest from European regulators in the sector, most notably resulting from the following:

- A "mirror trading case" involving a large European headquartered bank, concluded in 2017;
- An "Estonia case" involving a large European headquartered bank, concluded in 2018;
- The thematic review published by the UK FCA in 2019[11].

As a result of these, many firms are seeking to enhance their markets AML TM in a variety of ways:

- By sourcing additional data into the TM system, for example trade data (where previously there was only payment/ settlement data);
- By implementing further markets-specific detection typologies;
- By introducing new technology capabilities such as machine learning or network analytics;
- By establishing new teams dedicated to markets-specific AML TM alert review, investigation and disposition;
- By performing more "intelligence-led" analysis in addition to automated TM.

Regarding technology capabilities, there are a variety already implemented or planned (Figure) and there are differing views on the way forward.

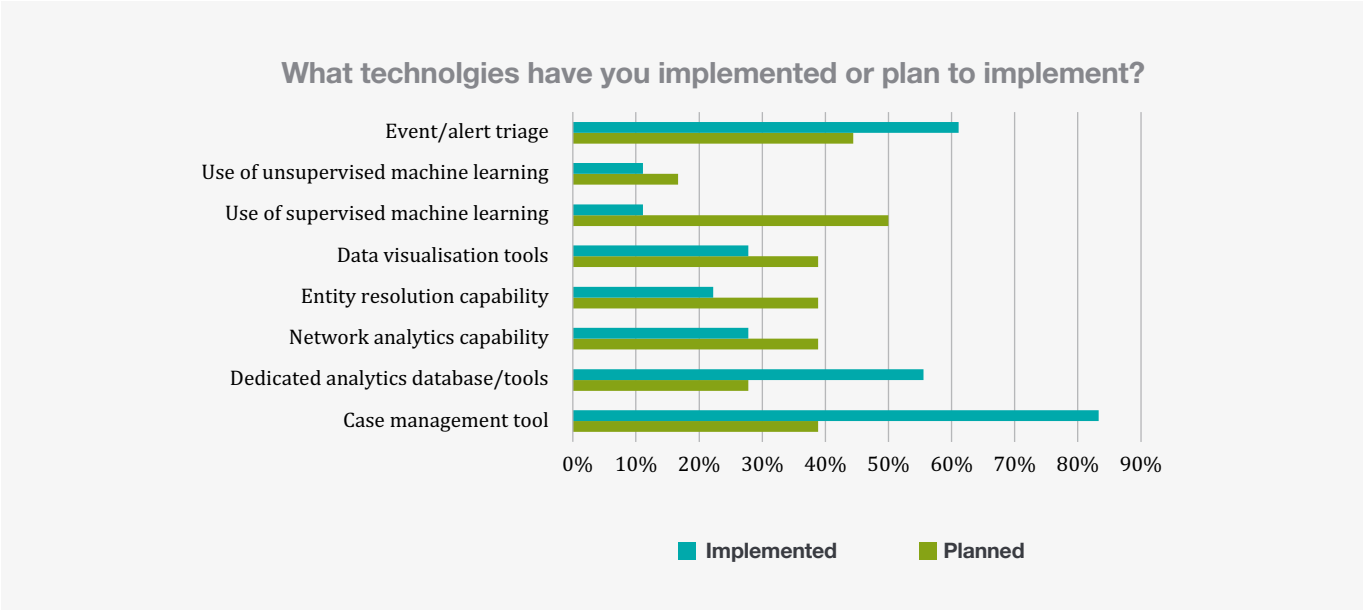


Figure 8: **Technologies implemented and those in plan to implement**

11 Understanding the money laundering risks in the capital markets, UK Financial Conduct Authority, 10/6/2019 (https://www.fca.org.uk/publications/thematic-reviews/tr19-4-understanding-money-laundering-risks-capital-markets)

What doesn't work?

It is instructive to first look at what doesn't work well. There are always exceptions, but in general the "classic" automated TM typologies taken from retail and business banking, and focussed on monitoring payments, do not yield productive alerts. These include things like change in behaviour (compared to historical activity), rapid movement of funds, structuring, single large value transaction and aggregate transaction value. The basic issue is that in a retail or business banking customers have fairly consistent, predictable behaviour over each month so activity that lies outside that norm becomes interesting to investigate. However, markets are much more volatile – behaviour can vary significantly across dimensions of time (i.e. volumes and values vary between one day and the next), product, trader and trading venue. As such, the classic typologies generally trigger on what is just normal fluctuation in trading, rather than genuinely suspicious. The only "classic" typology that appears to have some limited value for markets is payments to/from high-risk jurisdictions.

In response to this, there is increasing focus on a gradually growing set of "markets-specific" TM typologies[12], some already supplied by AML TM vendors and others developed on a bespoke basis. These have had mixed success: typologies like wash trading, pre-arranged trading and off-market pricing have in some instances produced good results whereas settlement focussed typologies like "free of payment transfers" have proved to be largely unproductive. With this in mind, attention has turned towards how detection is done, as opposed to purely relying on automated monitoring for specific typologies.

What does work?

About 20% of the firms we spoke to were getting some meaningful results with their AML TM. The techniques they employed included:

- Some automated detection typologies (as discussed above);
- Intelligence-led investigations;
- Machine learning;
- Network analytics.

We address each of these points in more detail, but the evidence suggests that there isn't a single approach or silver bullet. Instead, effective monitoring requires a hybrid approach of multiple techniques. Equally important are having sufficient skills to investigate and manage cases, and an operating model that supports continuous adaptation to new threat types and changing behaviour of market participants, as opposed to a static set of detection scenarios.

Intelligence-led investigations

An approach cited by several firms in our survey is to perform "intelligence-led investigations". As the name implies, these are not fixed rules that run in a system, rather they are ad hoc investigations based on a number of sources. These include internal referrals to the AML team, enquiries or feedback from regulators or law enforcement agencies, published cases of money laundering and terrorist financing using the capital markets, historical cases, risk-based sampling and data analysis or management information (MI). See case study 1 for more details, noting that the exact approach here will vary significantly between firms. In practice, each firm will need to have a customised programme of intelligence-led investigations tailored to the risk profile of its clients, the markets and venues on which it trades, the products it offers, and the actual patterns of trade activity.

12 See Appendix B

Case study 1: Intelligence-led analysis

Some of the firms we interviewed reported success with intelligence-led analysis. As opposed to rules-based monitoring which systematically runs the same rules across a firm's transaction data at regular intervals, intelligence-led analysis has the following features:

- **Human-led** – Analysis is driven by humans querying the data in an exploratory fashion rather than the machine running fixed rules.
- **Ad-hoc** – Analysis can be performed at any time.
- **Intelligence-led** – Analysis is based on pieces of intelligence, like a referral from the front office about a suspect client, an enforcement action on another bank or feedback from a Financial Intelligence Unit about a previous SAR filing.
- **Multiple dimensions of risk** – Analysis focuses on areas that present the most risk; for instance, when querying the data, there may be filters on client type to exclude low risk institutional counterparties, filters on the trading venue to focus on OTC trades and venues deemed to be higher risk, and filters on the instrument type, all of which makes the analysis much more targeted.

For example, intelligence-led analysis might focus on mirror trading as follows…

1. First identify the client population
2. Next filter on relevant securities or other financial instruments that could be used
3. Then filter on internally matched and OTC trades
4. Then look for statistically unusual counterparty pairs
5. Then, given a candidate set of entities with unusual behaviour, use network analysis to investigate each case, looking for potential hidden relationships between buyer and seller

From a regulatory perspective, relying entirely on this sort of ad-hoc approach is generally not deemed sufficient, so there is still a place for automated monitoring.

Entity resolution and network analytics

A number of firms are using or planning to implement network analytics, particularly as an investigation capability.

The idea of network analytics is to look not just at the behaviour of individual entities such as traders or clients, but to look at the relationships between them. These relationships may be transactional (for instance, counterparty pairs that trade frequently with each other) or based on more static data (for example, are two corporate clients part of the same group?).

Related to the concept of network analytics is entity resolution, i.e. determining if two individuals are actually the same person, or if two entities are actually the same corporation or under common ownership. Good entity resolution greatly improves money laundering detection, because all activity related to the same underlying entity is consolidated rather than fragmented.

There is clearly value in entity resolution to improve detection and in network analytics to aide complex investigations.

Enhancing AML TM with machine learning

Some banks are having success with their AML TM systems but are leveraging different data and using more sophisticated analytics, in particular machine learning. Details of this approach can be found in case study 2.

Case study 2: Machine learning

One bank has had success in enhancing traditional rules-based monitoring with machine learning techniques. For example, a classic TM rule like Change in Behaviour is typically not productive in the markets sector but can be enhanced to produce more productive alerts as follows::

1. **Focus on trade data rather than payment data:** Although money laundering technically only occurs when there are settlements or cash flows, it is the trade activity which is the best indicator of suspicious behaviour.

2. **Expand the feature set:** Rather than a simple "value and volume" approach, put additional features in the model like product mix, timing of activity and the notional trade value as well as the settlement value, plus details of the client sector, etc.

3. **Apply clustering methods:** Experiment with algorithms to identify the natural clusters of client activity using the feature set identified previously. Periodically regenerate the clusters, for example, on a monthly basis.

4. **Perform outlier analysis:** This is essentially peer group and historic feature comparison, looking for clients with activity that sits outside the clusters or the furthest distance from the cluster centres. Isolation forests have proven to be successful as an algorithm.

5. Also **apply supervised learning techniques** trained on historically productive* cases, to identify appropriate parameter settings for the enhanced feature set.

* When using supervised learning the definition or labelling of known positives to train and test against is critical to the success of an algorithm. In the case of AML we rarely have many or any known cases of money laundering within the historic data so using a definition of "productive" cases, i.e. those alerts that initially appear sufficiently concerning to warrant analyst time with in-depth investigation, provides a richer historic training set and therefore greater chance of a useful model emerging.

Steps 3, 4 and 5 enhance the models so that suspicious activity as opposed to merely statistically unusual can be identified.

There are still false positives, but there are also cases worthy of further investigation that do not get identified by the traditional "value and volume" rules.

Customer risk

When a customer is onboarded, or when customer details materially change, it is necessary to conduct "know you customer" (KYC) checks to understand the financial crime risk that the customer poses. There is then differential transaction monitoring of customers with different levels of risk, either by placing a customer with different risk levels in different segments, with different alerting thresholds for each segment, or by using a scoring factor in the calculation of an alert risk score.

In retail or business banking, typically there is a relatively small difference in monitoring between different risk levels of customers, for example a 10% or 20% lower alerting threshold for a higher risk customer such as a politically exposed person (PEP). However, in markets, customers carry much more significant differences in the level of risk they present. For instance, FX trading with a tier 1 institutional counterparty domiciled in a low-risk country presents a very low money laundering risk compared to dealing with retail brokerage or private wealth. Table 1 summarises views from the firms we surveyed about higher and lower risk customers.

Higher risk	Lower risk
Incorporated in high-risk countries (tax havens, FATF high risk list etc.)	Incorporated in low-risk countries
Unregulated in EU or UK or major market	Regulated in EU or UK or major market
Small cap corporations	Large financial institutions including banks, insurers, asset managers, broker/dealers
Complex corporate structures, special purpose vehicles, trusts, shell companies	Simple, transparent corporate structure
Brokers dealing with retail clients	Prop trading
Dealing in customised products	Dealing in vanilla products
High risk sectors (e.g. gaming, money services businesses, non-government organisations)	Public sector
Bearer shares in ownership structure, or nominee shareholdings	Corporations listed on a major exchange
Private individuals and private investment vehicles	Registered investment advisors

Table 1: **Examples of client types and attributes indicating higher or lower risk**[13]

In addition, the venue on which a trade is executed can be significant, with over the counter (OTC) trades being higher risk than trades through a recognised investment exchange.

It is important therefore to take into account the significantly different levels of risk in any AML TM.

Measuring success

In summary, a hybrid approach of significantly pared back traditional AML TM, enhanced AML TM using machine learning and intelligence-led investigations appears to be the best course of action for banks and other financial institutions looking to implement effective AML controls in the markets sector. These need to be underpinned by investment in technology capabilities, including network analytics. We discuss these different capability requirements in more depth in the next section.

With this more targeted approach we expect to see a much smaller number of alerts than with the traditional automated TM approach but a higher proportion of productive alerts and, ultimately, some SAR filings. As the volume of SARs for any given firm may still be low, some in the industry have suggested measuring success in terms of the escalation rate of alerts, i.e. the proportion of alerts that go on to the second level of investigation, instead. Ultimately, however, improved effectiveness will be expected to correlate with larger SAR filings across the sector.

The overall volume of money laundering in the markets sector going undetected is unknown, and there were mixed views on this point amongst the firms we surveyed as discussed in the previous section (see also figure 3). But overall, we can expect fewer alerts and fewer SARs than in other financial services sectors and as mentioned previously, higher in value when they do occur.

13 Please note the examples given in this table are those provided by individual firms and make generalisations based on specific experience. Applicability of these generalisations may vary by institution.

Technology uplift and data sharing are key

Capabilities required

In the previous section we discussed how a hybrid approach can yield meaningful results compared to traditional rules-based AML TM systems that generate very little or nothing of value. In order to implement this approach, a number of capabilities (both technological and people-orientated) are required. These are as follows:

- **Data lake**
  Many firms have implemented or are in the process of implementing a centralised data lake containing the data required for AML TM and for other financial crime functions such as Sanctions and PEP screening.

- **Analytics environment**
  An essential requirement is to have an analytics environment with query interfaces (e.g. SQL), data visualisation tools (e.g. Tableau, QlikView) and analytical programming tools (e.g. R and Python). This can be used for intelligence-led investigations, customer segmentation analysis, testing new detection typologies, and responding to regulatory inquiries.

- **Machine learning**
  A toolset supporting a range of supervised and unsupervised learning techniques is required.

- **Entity resolution and network analytics**
  A toolkit from a specialist vendor such as SAS, BAE Systems or Quantexa is often used to provide entity resolution as part of the automated AML TM and network analytics for complex investigations.

- **Skilled dynamic analysts**
  It is essential to build a team that has both data science skills and financial crime domain knowledge. The team needs to include people who are adaptive, creative and curious, as opposed to being staffed only with people who prefer to follow a standard *tick-box* process.

- **Senior management support**
  The above requirements need to have funding and support from senior levels.

More important than *what* is monitored is *how* it is monitored. The function responsible for AML TM needs to be adaptive and proactively search for emerging risks. Critical to this is leveraging a highly skilled team that understands both the financial markets and financial crime risks.

There are examples of firms implementing the same approaches, network analytics or machine learning for example, to solve the same problems with differing results. For some the approach has been successful but for others it has been less so. Whilst data will vary and data preparedness is important, the key differentiator is the people. Those firms that have seen success in these approaches attribute the people rather than the technique. Finding the right blend of skills and experience can be a challenge but ultimately provides the only way to apply advanced analytics across voluminous and highly contextual data.

Data sharing

> **"It is inevitable that we'll only see one side of the trades"**

A challenge identified by many firms is that the end counterparties of a trade are not always known. This can happen in a number of scenarios, including:

- A trade executed for a broker where the client is not identified;
- A trade executed on an exchange and settled via a central counterparty;
- An aggregated trade executed for an asset manager on behalf of several underlying beneficial owners.

Although the above scenarios are recognised as standard practice in the industry, what ideally needs to happen is a change in practice, either mandated by regulation, or broadly adopted as best practice, to require information about the identity of the end client(s) or counterparty to be shared. Early signs of this are emerging organically through the industry: some members of the International Securities Services Association are requesting that their clients share details of otherwise unknown end-clients with a significant (>25%) ownership of omnibus accounts. Whilst this poses an overhead for firms to query systems and identify beneficial owners it does provide greater transparency of end-clients. Some organisations are understood to be using elements of Artificial Intelligence to infer an end-client based on other activities on the account; for example, payments following a coupon or dividend distribution are usually direct to end-client accounts.

This challenge over end-clients is not new to financial crime teams, for example monitoring correspondent banking transactions where the ultimate originator was not always known. In that case a new SWIFT message type, MT202 COV, was introduced in 2009 to supply supplementary information to the MT202 payment message to identify the originator and beneficiary of funds. Given the complexity of markets infrastructure, to achieve the same outcome will not be straightforward but it is certainly possible. Ultimately a trade results in legal transfer of ownership of securities from one party (or several parties) to another, so the clients are certainly identifiable; getting this information to the right place is the challenge.

In the meantime, firms need to make best endeavours to identify clients and counterparties.

Centralised monitoring

Even if the end counterparties to all trades can be made transparent, individual firms can only monitor the trades and settlements that are booked in their systems. A more comprehensive view of client activity, and therefore more effective transaction monitoring, could be achieved if data and monitoring were centralised.

There are a couple of precedents for this. Firstly, in a sense this is already done for market abuse, whereby, in addition to firms performing their own surveillance, transaction reports are submitted to regulators under the EU Markets in Financial Instruments Directives (MIFID), enabling them to perform centralised surveillance and investigation.

Secondly, in The Netherlands an initiative began around four years ago to share financial crime data and intelligence between the four leading banks, the central bank and law enforcement. This required new data privacy legislation to be passed, and was a process that took some time to create. However, the pooled data has enabled both better proactive analysis and better investigations and ultimately is resulting in more criminal activity being identified.

Among the banks we interviewed, there was broad support for this type of approach but also a firm recognition that this is some way off in the future. As well as the challenges of overcoming data privacy restrictions (which are a particularly difficult when it comes to cross-border transactions), there is the crucial question of how this would be funded.

Many firms see the obvious solution being that there already exists a consolidated pool of transactional data lying with a single organisation per country that could perform centralised monitoring immediately. Through MIFID reporting obligations all trades of financial instruments are reported to and collated by a national regulator, the National Competent Authority. However, these regulators, whilst regulating firms' monitoring, do not have the mandate to monitor the data they collect for money laundering themselves.

Engagement from regulators and law enforcement

Feedback and engagement from regulators and law enforcement

A clear message from firms is that they would like to see clearer, more specific guidance on what they should monitor, and to receive feedback on SARs they have submitted (Figure).

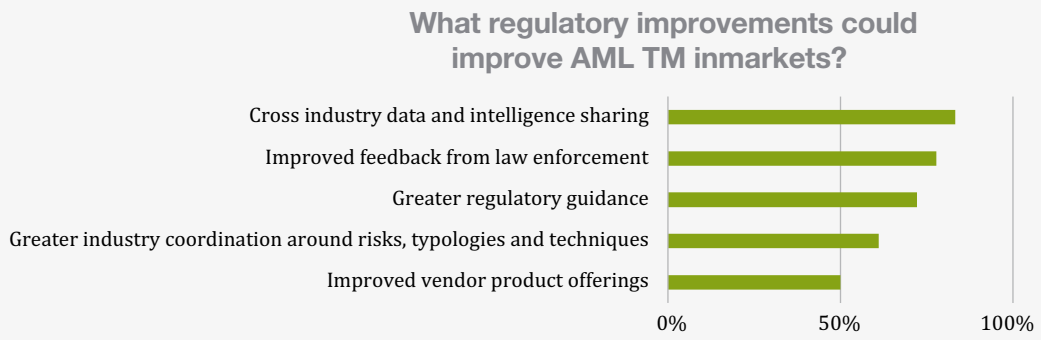


Figure 9: **Suggestions for regulatory support to help improve AML TM in Markets**

In particular, 85% of the firms we surveyed reported that they never get feedback on the SARs that they file. Of the firms that did, this was isolated to one or two specific markets.

One of the challenges with AML TM is that the regulator is the National Competent Authority (for example the FCA in the UK or the ACPR in France) but the recipient of the SARs is a different organisation, typically a Financial Intelligence Unit (FIU) within law enforcement (for example, the National Crime Agency in the UK or TracFin in France). This is different from market abuse surveillance where the body that administers the regulation and guidance is the same as the one receiving and investigating the reports (in this case STORs), so it is much easier to give joined up feedback to firms.

For instance, the UK FCA regularly publishes its *MarketWatch* paper, which often gives guidance on how firms can improve their market abuse surveillance[14] and on newly identified typologies for firms to be aware of. There does not appear to be a similar publication for markets-specific SARs submissions.

There does appear to be recognition from the public sector that greater focus is needed on markets' SARs. In May 2021 the UK FIU (the National Crime Agency) introduced a new SAR glossary code specific to money laundering through markets. This code will allow greater analysis of the volume of SARs submitted in the UK that are specific to the markets, a first step to better understanding of the issue across in one country.

14 See https://www.fca.org.uk/search-results?search_term=market%20watch

Regulatory perspectives

When researching this paper, we contacted a number of regulators and FIUs across Europe but the majority declined to be interviewed. Of the regulators and FIUs who kindly participated, there was limited specific guidance relating to markets but nevertheless some very valuable perspectives. The key themes from these conversations were:

1. **Get the basics right.**
   This includes having a documented risk assessment, audit trails of decisions and appropriate ongoing tuning of systems

2. **Senior management support.**
   Ensure there is the right level of senior management support for AML and sufficient funding

Law enforcement perspectives

From our discussions with law enforcement agencies, the following points were provided regarding the SAR regime in general (Markets sector and others):

- The SAR process works in the sense that ultimately criminals are prosecuted as a direct result of SARs filed by the private sector;
- Investigations can take a long time, typically 4-8 years;
- Most SARs are worthy of having been filed. One person we spoke to said 80% were good and only 20% should ideally not have been filed;
- Often the SARs themselves contain too much information, for example large numbers of transactions that are not suspicious when the focus should be on the transactions that are suspicious;
- Money laundering has been seen in the markets sector, but it is less commonly seen than for other sectors;
- One of the key challenges for law enforcement agencies when investigating financial transactions, and particularly markets' activity, is the difficulty of cross-border information sharing due to information privacy legislation which varies across countries;
- Given the huge volume of SARs submitted and the long investigation time, it is not feasible to provide feedback on them individually, but thematic feedback is possible.

Convergence between market abuse surveillance and AML TM

We previously discussed that, for many banks, the best source of SARs is referrals from the market abuse detective controls. In fact, at first sight, the two functions of trade surveillance for market abuse and AML TM are similar. Moreover, some regulators, notably the UK FCA, regard market abuse as a type of financial crime and therefore there needs to be the same governance and control standards for both functions[15].

This raises the question: should the two functions of market abuse surveillance and AML TM converge?

In fact, there are really two points here: 1. operational convergence and 2. technology convergence. All respondents saw opportunities for convergence but there were mixed views as to where this applied (Figure).

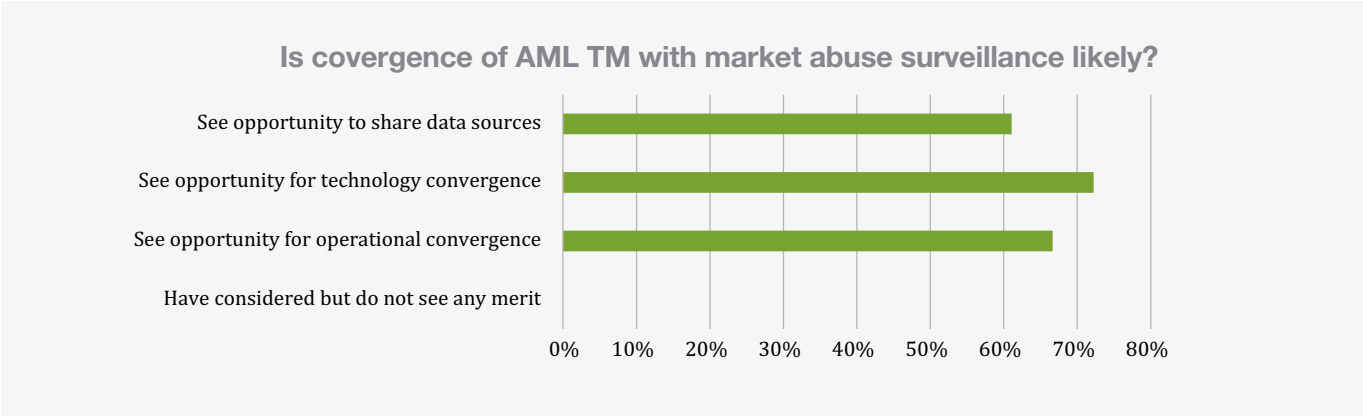


Figure 10: **View on convergence of AML TM with Market Abuse Surveillance**

15 Market abuse requires a dynamic response to a changing risk profile, UK FCA, published 13/2/2019 (https://www.fca.org.uk/news/speeches/market-abuse-requires-dynamic-response-changing-risk-profile)

Comparison between market abuse surveillance and AML transaction monitoring

Although these two functions appear very similar, if we look at them in more detail, there are a number of differences (Table).

	Market Abuse Surveillance	AML Transaction Monitoring
Who is monitored?	Employee and Client	Client
What is their motivation?	Opportunistic profit from white-collar workers	Systematic laundering of funds as part of serious and organised crime
What data is monitored?	Trades, Orders, Quotes, Communications (voice and text)	Trades, Payments (settlements)
Frequency of alerting	Daily	Daily/Weekly/Monthly
Typical data lookback period for alert generation?	Intra-day	Multi-day/Multi-Week
Example typologies*	Wash trading Front running Insider dealing Layering and spoofing Etc.	Wash trading Change in behaviour High risk geographies Free of payment transfers Etc.

Table 2: **Comparison between market abuse surveillance and AML transaction monitoring**

*These are a small set of the example typologies typically used but in the case of AML TM, not necessarily typologies that are proven to be effective in combatting the risks.

Operational convergence

Operational convergence is split into two functions: management convergence and analyst convergence.

A number of banks have implemented or are in the process of implementing these two functions at a management level, in other words, having shared line management and governance over the two functions.

Less common is convergence at the analyst level, by which we mean the actual investigations being performed by a shared resource pool. In most cases, although there might be a single manager with oversight of both functions, the alert investigations are still performed by two separate teams. That said, of the firms we surveyed, there was almost universally a close collaboration between the two teams.

Going forward, we expect to see more firms bringing these two functions together from a management perspective, and smaller firms starting to use shared resources for investigations. For larger firms, it is likely that investigations will continue to use separate teams given the differences between the two functions.

Technology convergence

Technology convergence is less clear cut. As shown in Table , although there are some commonalities, there are also a number of differences.

In particular, the underlying motivation for the activity is different: as a general rule, traders and clients who commit market abuse are opportunistic rather than inherently corrupt. Money launderers on the other hand will set up a scheme that is systematically intended to move proceeds of crime through the financial system. Therefore, patterns of nefarious behaviour are likely to be over significantly difference timeframes, and different in their design.

We are likely to see convergence in terms of shared data sourcing, for example data lakes supplying payment, trade, order and quote data. But there appears to be less of a case for shared analytics; it is likely that there will continue to be separate detection engines for the two functions, bearing in mind that, as discussed previously, in the future, the use of automated scenario based transaction monitoring is likely to be pared back for AML TM in markets.

Conclusion: Where next?

This paper has explored a number of considerations. Whilst the majority of firms report limited value from their existing AML TM capability, we have identified much that can – and should – be done to improve controls in a proportionate and risk-based manner.

Markets are complex and money laundering is difficult to find. The key point is that there is no quick fix solution of implementing a standard set of rules in an automated TM system. Rather investments in skills and technology are needed over a sustained period and hybrid approach of multiple techniques is likely to yield the best results.

As an initial roadmap to support improved monitoring for firms, we suggest the following steps:

Get the basics right	• Garner senior management support to establish a robust monitoring framework with continuous improvement embedded within it; • Develop an approach to understanding business as it evolves and mapping emerging inherent money laundering risks; • Establish clearly defined policy, procedures, oversight framework and governance structures.
Uplift technology capability	• Consolidate and connect data sources to the extent systems integration is possible; • Establish a flexible analytics environment, considering the nature and scale of operations; • Embed clear processes to add, amend and remove typologies and TM methods based on effectiveness, to enable quick and well-governed changes to take effect; • Implement entity resolution across the data and provide functionality to allow for network analysis and machine learning where valuable.
Upskill the team	• Build a small (proportionately), highly skilled team with domain experience and data analytics capabilities; • Invest in the team through professional development in markets understanding, analytical skills and financial crime knowledge
Optimise automated TM systems	• Apply custom analytics and/or machine learning techniques to improve detection typologies; • Focus on market-specific typologies that monitor trade activity; • Decommission scenarios that aren't productive.
Perform intelligence-led investigations	• This should take into account all dimensions of risk, including customer risk, market/venue risk, product risk, and geographic risk; • These will necessarily need to evolve and so procedures and governance should allow flexibility based on the understanding of risk at any given point.
Share knowledge and data with other market participants	• Support industry forums to build a common understanding of effective monitoring; • Share insight into anonymised cases and productive typologies or methods; • Support initiatives for data sharing, considering the data protection and privacy boundaries.

Across all those interviewed, a real desire to make improvements was consistently expressed and this coordinated effort across the industry is expected to bring change to this area over the coming years. We expect to see three stages of change:

Short term (1-2yrs): Improved monitoring and controls from the private sector is expected to lead to an increase in Markets specific SARs. In parallel, an increase in guidance and intelligence sharing based on a growing concentration of focus on Markets SARs both from private and public institutions will enable firms to accelerate enhancements to controls.

Medium term (2-5yrs): As we begin to see results from the increase in quality and quantity of Markets SARs we should expect to observe resultant criminal prosecutions emerge within a few years. Cases brought will provide the greatest feedback on criminal techniques used and provide a rich source of intelligence made public. We also expect to see instances of data sharing beginning to be trialled and potentially some central market monitoring being tested.

Long term (5yrs+): Within this decade we hope to see greatly improved data connectivity between firms using standardised protocols, both legal and technical, for efficient data sharing when needed having become the norm and whether the paradigm remains a distributed monitoring model or a centralised monitoring model, a leap in data coordination will allow far more powerful analytics and investigation.

Appendix A: Regulatory obligations in Europe to file SARs and STORs

The two relevant pieces of European Union (EU) legislation are:

1. The Market Abuse Regulation (MAR)[16]

2. The Money Laundering Directive (MLD)[17]

By definition, the first of these is law in EU member states whereas the second has been implemented into national law by individual EU member states. There are corresponding legal requirements in other European countries, such as the UK and Switzerland.

One key requirement of MAR is for firms to have systems and controls in place to detect either attempted or actual market manipulation or misuse of material non-public information (for example trading for a profit based on inside information). Suspicions and confirmed cases are documented as Suspicious Transaction and Order Reports (STORs) and sent to the relevant authority (usually the financial services regulator).

Similarly, the key requirement of the MLD is for firms to identify suspicious transaction activity that may indicate money laundering or terrorist financing activity. The obligation on firms is not to prevent or block this activity, but rather to submit a Suspicious Activity Report (SAR) to the relevant authority (usually a Financial Intelligence Unit in a law enforcement body). We note that in some jurisdictions, notably The Netherlands, there is a different requirement to merely report "unusual" activity rather than suspicious activity.

Historically, firms have regarded these as quite distinct functions but, as we discussed in this paper, some are beginning a process of convergence.

16 REGULATION (EU) No 596/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 April 2014 on market abuse (market abuse regulation)
(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0596)

17 DIRECTIVE (EU) 2018/1673 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2018 on combating money laundering by criminal law
(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L1673)

Appendix B: Examples of Markets-specific AML risk typologies

Typology	Description
Wash trading	A wash trade is when related investors simultaneously trade backwards and forwards with the aim to legitimize money of the proceeds of crime by moving it around and creating artificial volume in the market.
Mirror trading	Mirror trading disguises the transfer of high values of funds between countries and currencies by utilising the simultaneous purchase and sale of securities that have the same ultimate beneficial owner.
Trading account as bank account	This scheme uses a trading account to move the money in and out of it but with minimum trading activity on it, or a trading activity that is below the expected level for the amount of deposits and withdrawals. It is similar to using a trading account like a normal Bank account.
Money passing	Money passing is similar to wash trading except that the price is varying resulting in a net flow of funds between counterparties.
Account funding	A customer over-funding their margin requirements, only to be refunded at a later date to create an obfuscated flow of funds through an account.
Option premiums	This scheme uses equal and opposite options purchases such that a premium is paid and then paid back upon expiry in order to create an obfuscated flow of funds through an account.
Intermediation	Brokers are used to limit the sight that a firm has over the end-client making transactions and limiting the reach of customer due diligence.
Free of payment transfers of securities	The securities and custody scheme disguises the transfer of high values of funds between countries and currencies by utilising free-of-payment transfer of assets enabling clearing in different jurisdictions. This is a one-way transfer of securities
Debt issuance	A company uses an investment bank to transfer value across borders and appear clean through acting as both a loan issuer and a loan receiver with the bank acting as the onshore middleman.
Equity placement	Through issuing convertible debt an offshore company is able to allow a connected onshore investor to convert a low purchase value bond into higher value equity which can be sold to transfer funds into the onshore region.

Acknowledgements

We are grateful to AFME Financial Crime Working Group members who contributed their time and thoughts in producing this report.

The data in this report comes from interviews with 14 of those Members, and survey responses from a number of other members, representing a variety of geographical locations and business models.

www.afme.eu/Divisions-and-committees/Compliance

We are also grateful for the input of 3 European public bodies who agreed to be interviewed for this report.

Contacts

AFME

Richard Middleton
Managing Director
richard.middleton@afme.eu
+49 (0) 69 153 258 963

Louise Rodger
Director
louise.rodger@afme.eu
+44 (0) 203 828 2742

Giovanni Perrotta
Associate
giovambattista.perrotta@afme.eu
+44 (0) 203 828 2699

EY

Patrick Craig
Partner
Financial Crime and Forensics
pcraig@uk.ey.com
+44 (0)20 7951 2026

Tom Goodman
Director
Financial Crime and Forensics
tgoodman1@uk.ey.com
+44 (0)20 7806 9675

Jodie Forbes
Director (retired),
Financial Crime and Forensics

/ About AFME

The Association for Financial Markets in Europe (AFME) is the voice of all Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues.

We represent the leading global and European banks and other significant capital market players.

We advocate for deep and integrated European capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society.

We aim to act as a bridge between market participants and policy makers across Europe, drawing on our strong and long-standing relationships, our technical knowledge and fact-based work.

Focus
on a wide range of market, business and prudential issues

Expertise
deep policy and technical skills

Strong relationships
with European and global policymakers

Breadth
broad global and European membership

Pan-European
organisation and perspective

Global reach
via the Global Financial Markets Association (GFMA)

afme/
Finance for Europe

London Office
39th Floor
25 Canada Square
London, E14 5LQ
United Kingdom
+44 (0)20 3828 2700

Brussels Office
Rue de la Loi, 82
1040 Brussels
Belgium
+32 (0)2 788 3971

Frankfurt Office
Neue Mainzer Straße 75
Bürohaus an der Alten Oper
60311 Frankfurt am Main
Germany
+49 69 153 258 963

Press enquiries
Rebecca Hansford
Head of Media Relations
rebecca.hansford@afme.eu
+44 (0)20 3828 2693

Membership
Elena Travaglini
Head of Membership
elena.travaglini@afme.eu
+44 (0)20 3828 2733

Follow AFME on Twitter
@AFME_EU