We are delighted to present fscom’s **Fincrime Compliance Report for 2017**. The 2016 report brought to light some of the main challenges within payments compliance across a section of payment and e-money institutions in the UK. This time around, we are excited to bring to you not only a snapshot of compliance vulnerabilities in practice, but also insights on how firms have improved their compliance procedures in the last year and thus reduced their own regulatory, reputational, and financial risk exposure.

fscom is uniquely placed to evaluate and interpret relationships between regulation and practical implementation, and the subsequent analysis of results. With a wealth of compliance experience and a deep understanding of our client's business objectives, we work closely with our clients to uniquely grasp how regulations apply to them.

This report brings together such data analysis and professional insight with the objective of assisting clients and industry stakeholders by recognising industry trends, in order to enable firms to benchmark themselves against industry standards. We also anticipate that this report will assist with identifying weaker areas within internal compliance systems, and contribute to an understanding on how best to mitigate them.

Note that this report does not constitute the giving of advice, and fscom accept no liability, without limitation, for actions or outcomes based on findings or opinions within the report.

If you have any questions in regard to this report or how fscom can help you or your firm, please contact us and we will be more than happy to help you with your compliance needs and enquiries.

*The report and all data contained within are the property of FSCom Limited and may not be copied or reproduced without prior approval.*
## CONTENTS

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>BASIS OF PREPARATION</td>
<td>2</td>
</tr>
<tr>
<td>SCORING</td>
<td>2</td>
</tr>
<tr>
<td>MLRS 2017</td>
<td>3</td>
</tr>
<tr>
<td>AVERAGE CLIENT</td>
<td>4</td>
</tr>
<tr>
<td>INTRODUCTION TO DATA</td>
<td>5</td>
</tr>
<tr>
<td>PEPS AND SANCTIONS</td>
<td>8</td>
</tr>
<tr>
<td>RISK BASED APPROACH</td>
<td>11</td>
</tr>
<tr>
<td>CUSTOMER DUE DILIGENCE</td>
<td>14</td>
</tr>
<tr>
<td>MONITORING</td>
<td>17</td>
</tr>
<tr>
<td>TRAINING</td>
<td>22</td>
</tr>
<tr>
<td>MLRO</td>
<td>25</td>
</tr>
<tr>
<td>AML POLICIES AND PROCEDURES</td>
<td>27</td>
</tr>
<tr>
<td>CLOSING STATEMENT</td>
<td>31</td>
</tr>
</tbody>
</table>
BASIS OF PREPARATION

The data has been collected from audits carried out by fscom between October 2016 and November 2017. The information has been anonymised and collated to find trends and areas of both high and low risk in a number of payment, e-money institutions, challenger banks and cryptocurrency firms.

As audits typically report on negative findings only, positive findings have nevertheless been extrapolated by comparison with the previous year’s report and general comments from the audit findings.

The regulatory audit scope has changed in comparison with the 2016 report in that it no longer includes audit findings in relation to compliance with the Payment Services Regulations 2009 or Electronic Money Regulations 2011. This report focuses on audit findings in relation to compliance with the requirements of the applicable Money Laundering Regulations. This could account for some observed changes in trends between 2016 and 2017.

SCORING

In terms of risk scoring, the categories have been assessed with regard to the legislation and guidance applicable at the time of the audit.

Findings within our reports are categorised with a score ranging from 1 to 5. Findings rated as 4 or 5 were regarded as having the highest impact for the firm combined with the highest probability of crystallisation.

These high impact findings, individually or collectively, are in respect of breaches of the firm’s regulatory obligations, or where occurrence could result in significant client detriment.

Medium impact findings, rated 3, also pose some element of regulatory or systemic risk but are not deemed to be as significant as the high impact category.

Findings rated as 1 or 2 presented no significant regulatory issues but should nevertheless have been assessed and addressed by the firm after addressing any higher impact findings.

The risk scoring for issues found across the data set has been collated and then an average score per category created from these findings.
The past year has brought a great deal of regulatory change to the UK financial services market, and firms have been fully occupied in preparing to implement new solutions to meet their new regulatory obligations.

One of the main regulatory changes was of course the implementation of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, otherwise referred to as the MLRs 2017.

The MLRs 2017 brought into force amendments to the existing legislation, such as removing the automatic provision of simplified due diligence (SDD) for certain customers, changing the definition of politically exposed persons (PEPs) to include domestic individuals, requiring firms to provide written risk assessments including methodologies, and requiring EU member states to establish a central register of beneficial owners.

Firms should by now have updated and adapted their policies, procedures and controls to comply with these regulations, as a breach can potentially result in fines, criminal prosecution, or both, for firms and individuals.

If you have any questions in regard to this report or how fscom can help you or your firm, please contact us and we will be more than happy to help you with your compliance needs and enquiries.
WHO IS THE AVERAGE CLIENT?

Just over 56% of clients are authorised payment institutions (APIs), 30% are authorised electronic money institutions (EMIs) and other authorised entities, such as credit institutions and cryptocurrency firms, made up the remaining 14% of clients. The average client is located in London, with 82% of clients based within 50 miles of the City of London. Their average net assets were £7.75 million as per Companies House annual accounts.
INTRODUCTION TO DATA

As an introduction to the findings and information within, this section will give a general overview of the datasets used and initial results.

The chart below summarises our audit findings per compliance category, allowing an overview of the main compliance areas where we identified risks and their rate of occurrence, paired with the total risk averages per category. The statistics will be analysed in more detail later in the report, and the areas requiring the most, and least, improvements overall, will be highlighted.

We have witnessed general improvements in the overall risk rating, with last year’s overall risk figure at 3.70 (out of 5) being reduced to 2.65 in 2017. Even when discounting safeguarding from last year’s report (due to non-inclusion for this year within most audit scopes conducted by fscom), the 2016 average risk of 3.34 still stands higher than the current year’s average.
Comparisons between 2016 and 2017 reports also show a significant reduction in high impact findings. As previously mentioned, the risk scoring determines that issues given a 1-2 are low impact, 3 is medium impact, and ratings of 4-5 are high impact. The most notable change was that in 2016, 37% of findings were high impact, whereas in 2017 this figure had reduced to 18.6%. There are several factors to consider that rationalise the improved scoring % stated above. Firstly, some firms are progressing year on year by implementing more effective procedures, systems and controls, which remediate previous years issues identified, which is then reflected in the average scores documented in our audit reports. Secondly, we as a firm have aligned our report formats and weighting allocated that impact some findings for consistency in our scoring methodology allocated per finding. Finally, the types of firms we conduct the audits on, typically are those that have resource to allocate to external consultancies for advisory and compliance projects to enhance internal functions and processes. These culturally compliant firms could distort the average scores allocated per section within this report if it assumed they can be directly transferable to the whole payments and e-money sector.

<table>
<thead>
<tr>
<th>Year</th>
<th>Low Impact</th>
<th>Medium Impact</th>
<th>High Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>33%</td>
<td>30%</td>
<td>37%</td>
</tr>
<tr>
<td>2017</td>
<td>43.5%</td>
<td>37.9%</td>
<td>18.6%</td>
</tr>
</tbody>
</table>

Despite a rise in issues found, the data set used was also expanded. The resulting number of issues per client was around 10% less compared to the increase in data, which shows less findings were identified in 2017, per client, per audit.
The UK’s national risk assessment of money laundering and terrorist financing 2017* has categorised both money laundering (ML) and terrorist financing (TF) risk for MSBs as high. The 2016 report showed ML risk for MSBs as medium, so this is a significant change.

These types of businesses have experienced de-risking, as they have been considered targets for ML and TF due to their cash intense business model as well as being seen as having significant challenges with their anti-money laundering (AML) and counter terrorist financing (CTF) controls. This approach has displaced ML and TF criminality to more vulnerable areas of financial services, and at times pushed the illicitly inclined firms to avoid any contact with the AML/CTF regime. It is vital for MSBs to consider their responsibilities towards the UK financial system and ensure that their compliance procedures, policies and controls are their first and most important step to lower this risk to legitimate MSB firms.

In contrast, e-money services such as certain prepaid cards are considered in the same assessment to have the potential to become high risk. However, due to the monetary limits for storage and transactions, they are not considered considerably attractive means of illicit transfers of funds.

In the next section, the report will go into more detail regarding particular issues found that payment services providers (PSPs) and MSBs could evaluate and improve to reduce their business, compliance and financial risk exposure.

**PEPS & SANCTIONS**

**Regulatory requirements:** Firms must have risk management systems to determine whether a customer or beneficial owner is a PEP or not, obtain and record senior approval of establishing business relationships with PEPs, take reasonable measures to establish source of funds and source of wealth, and conduct enhanced due diligence throughout the business relationship.

![Diagram showing risk categories:]

- 33.5%: Fuzzy logic not consistently effective or not functional
- 30%: Lacking an effective sanctions screening procedure
- 23.5%: Procedures not consistently effective
- 6.5%: Escalation and quality control measures not effective
- 6.5%: Data or testing issues

**Fuzzy logic not consistently effective or not functional. 33.5%**

In the majority of cases, the firms did not utilise fuzzy logic at all, and in the remaining cases the fuzzy logic test did not yield consistent hits, due to restrictive fuzzy logic rules or variables set by either an external supplier or the firms themselves.

**Lacking an effective sanctions screening procedure. 30%**

The firms affected have issues with their screening procedures, such as not screening certain names, clients or transactions. Certain firms also fail to re-screen names within a satisfactory time frame, or before conducting transfers.
Screening measures not consistently effective. 23.5%
Within this category, sample testing failed in one or more cases. It was also found that evidence of PEP & sanctions searches was not retained within the client file. Note that consistency is the main issue for this category; in most cases related to the system not identifying a well-known PEP.

Data or testing issues. 6.5%
Firms either did not identify PEPs or sanctions due to an external provider experiencing problems with their database or lacking data, or the system did not have the capacity to screen individual names.

WHAT DID FIRMS DO DIFFERENTLY?

In 2016, the overall risk rating for this category (the average figure) was 4.42. In 2017, this has been reduced to 2.64, which is a significant reduction in severity of issues.

Why is this? – having identified screening issues onsite with firms, we also educate what firms can do to monitor the effectiveness of their own processes. This results in new ongoing testing processes being developed and implemented with some firms to ensure they are effective rather than assuming a process works well, indefinitely. Also, we’re seeing an increase in resources being allocated to external specialist vendors who provide an effective and established screening solution which reduces our findings within this category during an audit. Whilst the risk average was reduced, the number of firms experiencing issues with PEPs and/or sanctions, has increased by almost 10% from 73.7% in 2016 to 83% in 2017.

Why is this? – We’re seeing a shift from an in-house manual or ineffective automated screening process, by some firms, to outsourcing its entire screening process to an external screening vendor. However, as much as this can be considered a positive move, utilising a specialist vendor for a key process is expensive with some firms agreeing a basic screening package that doesn’t fulfill all of our testing elements, such as the inclusion of fuzzy logic testing. In addition, the client applies the screening criteria based on their own risk appetite regarding when and what is screened which also impacts the effectiveness of the procedure and potential scores allocated to an issue identified during our testing.

Some firms appear to be solely focused on being associated with a reputable screening vendor rather than implementing a complete and effective product. This association is then viewed externally by stakeholders as a positive move but key to a successful screening provider is a specialist integration.

Out of the matters found, 19.5% of these were considered high risk, which is the fourth highest of the categories identified.

The impact of 4MLD on this element of the audit scope as many of the well-known screening providers already included home based PEPs within their screening scope prior to June 2017 so were already compliant from this perspective.

Escalation or quality control measures not effective or appropriate. 6.5%
These results showed a non-existent Q&A control, with a lack of oversight of approvals. Also, this category identified cases where oversight was present, but individuals lacked appropriate experience within the relevant field.
PEPS & SANCTIONS CONTINUED

The MLRs 2017 introduced an important change to the definition of PEPs, with domestic individuals of a prominent public position now considered to fit into this category.

Where the MLRs 2007 stated that PEPs should not be considered on a risk gradient, the MLRs 2017 have changed that.

Although the presence of PEPs should trigger enhanced due diligence (EDD), the FCA has published guidance on how to treat persons of various positions, and how to differentiate the risks that local, EEA and non-EEA PEPs pose to firms.

It is also vital not to refuse PEPs as clients as a matter of policy, as this is against the 4MLD provisions.

The Government also brought into force the use of unexplained wealth orders in 2017, which highlights the importance for source of funds and source of wealth in investigations conducted by the National Crime Agency (NCA) and Financial Intelligence Units (FIUs).

Accordingly, it is vital for firms to have set policies and procedures on the source of wealth and source of funds that can be accepted, and the verification of such information.

There is a general lack of available guidance on this issue, which doesn’t mean it is of less importance.

Quite the opposite, as firms need to carefully consider the risk they expose themselves to by not setting clear guidelines internally.
Regulatory requirements: A relevant person must take appropriate steps to identify and assess the risks of ML/TF to which the business is subject – this includes risk factors such as customers, jurisdictions and geographic areas, products and/or services, transactions and delivery channels.

Not conducting an effective risk assessment. 28.5%
Findings revealed risk assessments that for example did not consider PEPs, location, jurisdictions for payments, product risk, intended use of relationship, or that had non proportionate risk scoring which resulted in all clients being classed as low risk.

Enhanced due diligence issues. 20%
Not recording senior management or MLRO approval, not conducting EDD on certain high risk clients, accepting insufficient documentation for higher risk transactions or not requesting evidence of source of funds/wealth from the client. Also, clients were retained that were outside of risk appetite, but not subject to EDD.
Not documenting the RBA or some of its variables appropriately, 14%
For example, the geographic risk assessment was not documented appropriately and in cases outdated, or the clients risk scores were not linked to their CRM accounts, nor were they flagged as high-risk clients.

Risk assessment for certain types of entities/clients/agents not effective or missing, 11%
Identified cases where agents or underlying customers did not have a documented risk assessment, but in an equal amount of cases, firms had not applied an effective risk assessment on certain types of clients or industries.

WHAT DID FIRMS DO DIFFERENTLY?

Even though this is the highest risk category overall, in 2017, the average score has been reduced to 3.11 from 3.73 in 2016, which indicates an improvement in how firms implement their risk based approach.

**Why is this?** - The average score for this category has reduced slightly, however is still higher than average and accurately reflects the issues we continually see on-site.
Having witnessed an increased implementation of more effective risk parameters in theory, the execution of the risk assessments still requires improvement. Issues that firms frequently experience are effectively weighting risk parameters, inclusion of a variety of relevant risk categories for both private and corporate matrices and completing the risk fields for a full assessment.
31% of issues were considered high risk, which is the highest occurrence seen within any section.

**Why is this?** Taking into account the changes with 4MLD mid-year, some firms were not proactive in conducting a review of their own internal assessments, which accounts for some of the increased scores allocated in this section. Instead, some firms would wait until the annual review before updating and noting changes within the year.

Some clients not reassessed or missing risk assessment, 8.5%
In 2/3 of cases this was an issue stemming from accounts opened before a certain system or process was adopted. Remediation of risk had not been performed appropriately at the time of audit. Other customers had no risk assessment saved in their client files.
RISK BASED APPROACH CONTINUED

This year, the MLRs 2017 removed blanket risk classifications such as SDD, which applied to certain firm types such as authorised firms, to focus on bespoke risk evaluations of each customer, based on an understanding of CDD information.

Ultimate beneficial owners must now be identified for all firms (apart from, in most cases, entities on certain regulated stock markets).

The methodology behind all risk considerations must be recorded, and risk assessment should take into account the variety of clients and their equivalent difference in risk.

Firms have an obligation to include what risks their various products pose to the relationship, and this should be included in all cases.

It is also worth pointing out that a risk based assessment done well can reduce the burden of excessive monitoring on a firm’s compliance department, as a result of risk misclassification.

The Joint Committee of the three European Supervisory Authorities (ESAs) published their Final Guidance on Risk Factors in June 2017. It equips firms with the tools they need to appropriately understand and benchmark themselves in terms of risk approach, compared to what is expected from them by the supervisory authorities.
Regulatory requirements: To identify and verify customer and ultimate beneficial owners, understanding the business relationship and to conduct ongoing monitoring of the relationship. Breach of the requirements could result in a fine or up to 2 years in prison.

Documentation issues: incomplete records, inconsistent records, lacking translation. 29.5%

In many instances, customer files did not contain sufficient CDD documents. Translation of documents was also an issue. Missing certification or documented approval by compliance or senior management was also lacking.

Not consistently effective CDD procedures. 20%

Several firms had inadequate or non-existent KYC profiles for their clients for the samples reviewed, which indicates ineffective CDD procedures. Failure to identify and verify UBOs and directors was also found in cases.
Insufficient client information obtained (current). 6%
For new clients, some firms did not obtain purpose of relationship, transaction volume, jurisdictions of payments or other variables. In isolated cases, documentation obtained for new clients did not meet an appropriate level of verification.

Insufficient client information obtained (historic). 14.5%
Many firms did not hold sufficient client information, such as general CDD documents and the nature and purpose of the relationship. Verification was lacking in historic accounts as well as documentation requested and obtained in general.

CDD refresh/review issues. 12%
No review procedures implemented or scheduled, or alternatively not completed at time of audit.

WHAT DID FIRMS DO DIFFERENTLY?

CDD is a category which has seen a significant improvement since 2016. The risk score was reduced from 3.52 to 2.88 and the occurrence decreased from a considerable 89.5% to 74%. However, this means that 3/4 of firms still face CDD issues.

Why is this? – Firms have generally improved year on year partly due to the increased variety in solution providers offering cost effective onboarding solutions that utilise technology, ensuring the starting point for CDD has improved. Some of these external vendors also offer CDD refresh services which contribute to an effective and complete solution ensuring client data is kept up to date on an ongoing basis. However, this is at a cost.

Companies House has also partly assisted the competition in the sector by offering free UK data on its platform. However, the ease at which foreign data is available remains a problem in many jurisdictions, which increases costs and the resource taken to update client data to an appropriate standard. This results in some foreign client data being out of date due to the lack of information readily available to update CDD and to comply with its obligations.

27% of issues were considered high risk, which is the second highest, together with the MLRO category, which also has 27% high risk issues.

Due to the sector being very competitive and to enable a firm to generate reasonable revenues and profits, typically firms have significant client lists. These client lists are also deemed a key asset for any firm when valuing a business or considering additional external investment. Therefore, to maintain current client data, ensuring it is up to date, can be overwhelming and take significant resource on an ongoing basis, which some firms simply don’t have.

Simply for some firms, once the initial CDD is completed and the account is signed off and is transacting, some firms believe their CDD duties have been completed and ignore that changes can occur within any client, which may then require further CDD obligations.

Insufficient client information obtained (current). 6%
For new clients, some firms did not obtain purpose of relationship, transaction volume, jurisdictions of payments or other variables. In isolated cases, documentation obtained for new clients did not meet an appropriate level of verification.
CUSTOMER DUE DILIGENCE CONTINUED

There is no doubt that customer due diligence measures and record keeping provisions are closely linked.

As seen, adequate record keeping of CDD documentation used in the identification and verification process is lacking in many cases.

Retaining documents used for CDD purposes is not an optional approach, and the lack of such documentation could prove a hindrance where a suspicious activity report (SAR) is or has been initiated, if the individual or customer cannot be suitably identified.

Issues with CDD can be rectified with a clear tone from the top which promotes strict procedures and a strong compliance culture.

With the rise of fintech and technology such as electronic identity verification (EID), it may seem to firms like obtaining sufficient CDD is only a click away.

However, it is vital for firms to fully understand the data EID checks are based on. To be relied upon, the data should be from multiple sources and span over a time, and a successful EID check is also not a safeguard against impersonation and/or fraud.

As always, it is imperative to conduct CDD with a risk based approach in mind, as higher risk customers are expected to face a higher level of CDD scrutiny than medium/low risk clients.
**MONITORING**

**Regulatory requirements:** To conduct ongoing monitoring of the relationship and to apply scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the relevant person’s knowledge of the customer, the customer’s business and risk profile.

<table>
<thead>
<tr>
<th>TRANSACTION MONITORING</th>
<th>ONGOING MONITORING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non effective TM system / lack of security</td>
<td>Not monitoring changes to clients</td>
</tr>
<tr>
<td>Limited CRM functionality</td>
<td>Monitoring procedure is not robust</td>
</tr>
<tr>
<td>Backlog of TM alerts</td>
<td>Periodic CDD review issues</td>
</tr>
<tr>
<td>High number of false positives</td>
<td>Issues with CDD data for purposes of TM</td>
</tr>
<tr>
<td>Other</td>
<td>Other</td>
</tr>
</tbody>
</table>
TRANSACTION MONITORING

Non-effective TM system / lack of scrutiny. 48%
Firms were missing real-time monitoring, experiencing a backlog of post-event monitoring alerts and lacking effective rules. Certain variables such as frequency, volume and size of transactions were at times not considered.

Limited CRM functionality. 26%
The CRM system was found to not generate management reports or automated alerts, not include client risk rating, and was in cases found to not link KYC profiles to alerts. In isolated cases, the CRM system was not able to quarantine suspicious transactions.

Backlog of TM alerts. 7.5%
Significant backlogs of high risk alerts, including PEPs and sanctions alerts. Aged alerts identified which had not been resolved appropriately and in a timely manner.

High number of false positives. 7.5%
TM system not configured accurately, resulting in a considerable amount of sale positives, which hampers the effectiveness of the compliance department.
WHAT DID FIRMS DO DIFFERENTLY?

Overall, monitoring risk has been reduced by almost 1.03, with 2017’s score of 2.75 being significantly lower than 3.78 in 2016. Transaction monitoring as a stand-alone category holds a 2.75 risk score, which is still a positive trend in direct comparison. Transaction monitoring issues are uncomfortably common, at 87% of firms.

Why is this? – Originally for some firms, they have utilised white labelled mass market systems that typically didn’t suit their business model as the functionality was limited and intentionally designed to be generic rather than bespoke for a certain industry or business type. This coupled with the difficulties and cost faced in requesting IT development from the CRM system vendor to better suit the client’s own business model resulted in ongoing functionality and development restrictions.

We have noted a shift by firms to more effective CRM system solutions due to improvements in technology and functionality and more options available with new entrants competing for a market share in a lucrative sector. However, although base CRM systems have improved, to make them an effective and complete solution coupled with clawing back a return on the vendors significant investment, vendors have pricing models and sell extras such as transaction monitoring bolt-on tools. This then creates an additional cost barrier for an immediate effective solution with a view by some firms to building their functionality over time to reduce the cost impact.

For other firms, with more resources, they remove the reliance on the expensive middle man, (the CRM system vendor) by typically recruiting and retaining their own in-house IT development teams who design, build and maintain their own bespoke CRMs or update existing white labelled systems to better suit their business models. This IT function does come at a cost but can add significant value to a firm and can provide significant competitive advantage within the sector. We have noticed more firms having an established in-house IT resource that can react quickly to requests by compliance and be proactive when streamlining business processes. The rationale for some ongoing transaction monitoring issues relates to source information. As new automated processes are introduced and plugged into CRMs, they rely on complete and reliable data. If this data isn’t completed, the process becomes ineffective. To remediate this requires both time and personnel resource.

18.5% of issues were considered high risk within transaction monitoring, which is high. However, the low 5% rate of high risk issues within ongoing monitoring has reduced the overall figure of high risk issues to 11.75%.
Not monitoring changes to clients. 35%
Many firms were found to not monitor client changes at all. This was in the majority of cases due to the lack of system functionality, not activating the function, or not having added clients to the monitoring system.

Monitoring procedure is not robust. 20%
The TM system had conflicting risk ratings or the system had not been assessed for functionality. Some firms were found to deal with shell companies due to not applying a robust TM process.

CDD periodic review issues. 20%
Client file lacking clarity as to whether or not the review has been completed, some clients falling outside the refresh procedure or no flag to alert that a review is required. Some firms reviewing clients every year regardless of risk rating, which is unnecessary.

Issues with client data for purposes of TM. 15%
Findings include unverified profile data, lacking system to maintain customer KYC data and KYC profiles which could not be amended on CRM after account creation.
WHAT DID FIRMS DO DIFFERENTLY?

Ongoing monitoring as a stand-alone category is lower risk overall compared to transaction monitoring, at a 2.40 risk score.

As mentioned, ongoing monitoring also only has a 5% high risk issue rate, which is the lowest of all categories within the report.

Why is this? – The change in early 2015 for Companies House to make data available for free and offering the ‘follow’ function has contributed to firms being more proactive with maintaining their client data in the UK. The difficulties firms still face is allocating resource to complete these huge CDD refresh projects as they are significantly resource hungry from a personnel and time perspective. In addition, foreign jurisdictions aren’t as generous as the UK and still make CDD acquirement difficult on an initial and ongoing basis.

With an occurrence of 74%, this also reduces the overall score for monitoring. Last year’s rate of monitoring issues were at a high 84%, which has been marginally reduced to 80% overall.

Failing to identify linked transactions, applying generic transaction monitoring rules, or not completing the customer profile correctly all result in an ineffective transaction monitoring (TM) system.

The TM system should also include provisions to conduct risk-based monitoring, which is lacking in many cases. Where the customer profile is in some way inaccurate, the efficiency of TM will also be reduced.

TM can give a firm a clearer view of customer behavior and profile, and when done right, a firm should be able to use the system to more easily distinguish payments conducted that are not in line with the customer’s prior behaviour and profile.

As it is a regulatory requirement to monitor customer accounts for changes, e.g. when new directors are appointed or a change of ultimate beneficial owners, failing to apply an effective ongoing monitoring solution is a regulatory breach.

Additionally, should aspects of the customer profile change, the risk rating may no longer be accurate. Not observing and reacting to such changes can lead to a firm unknowingly retaining clients outside of their risk appetite.

Challenging a customer to provide additional documentation in light of changing circumstances may be a delicate matter, but it is vital to remain focused on the potential negative consequences of not doing so.
**Regulatory requirements:** A relevant person must ensure its relevant employees are made aware of the law relating to ML and TF, and regularly given training in how to recognise and deal with transactions and other activities or situations which may relate to ML/TF.

- Ineffective AML training
- Procedures not in place to ensure all staff receive appropriate training
- AML training within 12 months could not be evidenced for some staff
- Some staff had not received AML training
- Other

**Ineffective AML training, 52%**
Assessments of AML knowledge was often insufficient or not broad enough, and otherwise not assessed effectively due to questions being too easy. In other cases, the AML training was not bespoke to the business and was found to be too general in content.

**Procedures not in place to ensure all staff receive appropriate training, 22%**
Firms showed evidence of lacking in role specific training, such as MLRO and systems training. In other instances, procedures were not in place to ensure regular training was received by staff.
AML training within 12 months could not be evidenced for some staff. 17.5%
Some staff only had records showing they had been trained outside of the 12-month interval, and some firms were missing logs to evidence staff training or the log simply was not updated.

Some staff had not received AML training. 4.5%
In very few cases, the staff had not received any kind of AML/CTF training. In one instance, almost 1/3 of staff had not received appropriate AML training.

THE FOURTH MONEY LAUNDERING DIRECTIVE - TRAINING

2/3 clients audited after the 26th of June 2017 had not updated their AML training to reflect recent changes found in the 2017 MLRs.

After the much publicised implementation of the 4th Money Laundering Directive, firms were expected to have amended internal procedures and training to reflect this change.
WHAT DID FIRMS DO DIFFERENTLY?

Training has seen an overall negative movement in 2017. The risk score has risen overall from 2.45 to 2.63, and the occurrence has risen by 14% from 60% to 74%.

12.5% of issues were considered high risk, which is far from the highest at fifth position. However, training is such a vital part of a firm’s controls that it should be expected to be a high priority and as such 12.5% is a relatively high number.

In terms of general AML training, many firms seem to adopt an AML training programme that typically covers the basics well, but year on year developments within the training programmes are minimal so no further learning is developed per employee and typically no relevant case studies to highlight key points and obligations are consistently used. Training for some firms seems to be executed as a tick box exercise rather than a risk mitigation process to reduce the firm’s exposure to being involved in ML/CTF.

More recently, it has been noted that firms are allocating more resource to educating key senior staff members with external certification such as ACAMs and ICA courses to further develop knowledge and experience in the industry. This knowledge can then be redrafted into in-house training packages to complement existing training programmes.

In terms of 4MLD, the majority of firms implement an annual training programme with their employees and with 4MLD being introduced mid-year from June 2017, many firms had already conducted their training for 2017 and would wait until their next formal annual training before including an overview of 4MLD.

Some firms were proactive by holding an interim training seminar to provide, at the very least, an awareness of the key changes to the MLRs 2017 or senior personnel attended external briefings which then allowed this information to be cascaded throughout their firm.

Due to the hype around 4MLD and the vast amount of commentary on social media and publications, thankfully there was a lot of information and opinions on 4MLD. In fscom’s experience, it was noted in the majority of cases, it was senior personnel within the compliance sector who were more familiar with the 4MLD changes, but this was not consistent throughout the firm both at senior level in other departments and at a junior level.
**MLRO**

**Regulatory requirements:** An individual in the relevant person’s firm must be appointed as a nominated officer.

- **36.5%** MLRO not independent.
  The MLRO was found to be the managing director, owner, board member, COO or an ultimate beneficial owner of the firm.

- **27.5%** MLRO annual report insufficient or non-existent.
  The MLRO had either not prepared reports for the board on an annual basis or had only prepared a brief overview of functions which did not assess the functionality of AML/CTF controls, or had not prepared any report at all.

**Average Risk:** 3.09

**Occurrence:** 35%
No dedicated MLRO at time of audit. 18%
The MLRO was found to be either an individual with another role within the firm, or there was no MLRO employed at the time of audit.

WHAT DID FIRMS DO DIFFERENTLY?

In last year’s report, the MLRO category had an average risk score of 3.3 and affected almost 70% of firms. In 2017, the number of firms experiencing issues with the MLRO function has halved to only 35%, and the overall risk has decreased to 3.09. However, this is still the second highest risk score of all categories within the audit scope.

Why is this? – There is a relatively simple explanation. Many firms are struggling to source suitably experienced and qualified compliance staff. In some instances, the MLRO function is found to be held by a member of the senior team with no specific AML experience or firms had no dedicated MLRO at all. This inconsistency of the MLRO function also plays into a firm’s inability to set up sufficient monitoring statistics or board reporting.

Additionally noted was the rise of a number of interim MLRO functions held by consultants with a view to setting up good systems and assist in the recruitment process. This has varying levels of success dependent on the consultant or organisation. However, it shows how key the recruitment of this role is to build out significant compliance function fit for a scaling business.

A risk of not having an independent MLRO, is that management tasks relating to AML/CTF issues take a backseat compared to the running of the business, which may skew the approach to favour profit over compliance.

In smaller businesses, not having an independent MLRO may be mitigated somewhat by the size of the firm.

However, it is imperative that the MLRO, whoever this may be, has in depth knowledge about the firm, the regulatory landscape and the seniority to take ownership of their tasks, including SAR reporting and communications with financial intelligence units.

The MLRO function is vital in larger businesses, to keep the SARs procedure in line with regulations, and the individual appointed should be fit for the role and possess appropriate knowledge of what is required of them.

A vital task for the MLRO is to keep up to date with regulatory requirements, to ensure that firms have adequately prepared for new developments and that AML/CTF policies and procedures are updated where required.
AML POLICIES & PROCEDURES

Regulatory requirements: A relevant person must establish and maintain policies, controls and procedures to mitigate ML/TF risk, and these policies must be regularly reviewed and updated.

INTERNAL DOCUMENTS

- Policies contained issues requiring amendment: 48%
- AML policy contained minor issues requiring amendments: 26%
- Policies not updated to reflect new procedures or regulation: 7.5%
- Other: 18.5%

RECORD KEEPING

- Insufficient SAR information recorded internally: 32.5%
- Some SAR information not filed securely: 14%
- Insufficient SAR information for external submission: 11.5%
- No resolution of PEPs & sanctions hits documented: 9.5%
- Other: 32.5%
**WHAT DID FIRMS DO DIFFERENTLY?**

Within the internal documents category, the risk was the lowest within the report at 1.95 per issue as average. The number of firms experiencing issues with their internal documentation such as policies was 74%.

**Why is this?** Similarly, to the training issues identified and noted earlier within this report with 4MLD that was introduced mid-year, policy documents and firm manuals are also typically reviewed on an annual basis. Therefore, for some firms, the review process had occurred in 2017 for the 2016 period and it would be several months before the significant 4MLD amendments would be implemented as part of the 2017 review, conducted in 2018. Certainly, towards the end of 2017, many firms had commenced their preparation for the PSD2 reauthorisation process, ensuring policy documents were up to date earlier for the FCA’s review once application had been submitted, which encouraged firms to update policy documents slightly earlier knowing they would have to pass FCA inspection.

There were only 4.75% of high risk issues within this specific category. Although there were many findings, most were considered to have low to medium impact on the business.

Typically, issues linked to policy documentation are deemed as a lower risk issue regarding impact to the firm and possible client detriment. This statement though is crosschecked with on-site testing in relation to the effective implementation of the relating procedure. If both policy and procedure are absent, then within our reports the failed procedure gets a higher risk rating allocation compared to the lack of a relating policy being documented. As a leading UK consultancy, fscom has access to a vast catalogue of source materials, experienced and knowledgeable professionals, Associations, the Regulators and law firms, so typically can provide improvements to any policy documentation. Therefore, for most compliance audits, minor recommendations are always going to occur as these businesses and best practice will continually evolve.

**Policies not updated to reflect new procedures or regulation. 7.5%**
The policies were not updated to reflect amended firm procedures following the implementation of 4MLD.
RECORD KEEPING

Insufficient SAR information internally. 32.5%
SAR logs did not contain status of SAR, reference number, if consent was required, linked SARs, summary of suspicion, if MLRO had reviewed or not. Other cases showed that SARs were not documented within the SAR log at all.

Some SAR information not filed securely. 14%
SAR information did not have restricted access, or was stored in a central location. Instances were also identified where reporting staff members received hard copies of the report. This increases the risk of committing a tipping off offence.

Insufficient SAR information for external submission. 11.5%
Reports were lacking details on criminal property, SAR subject, bank details and firm overview. This reduces the effectiveness of the SAR process.

No resolution of PEPs & sanctions hits documented. 9.5%
The resolution was either not documented at all or not consistently documented within client files.

WHAT DID FIRMS DO DIFFERENTLY?
The overall risk for the record keeping category is 2.14 and the occurrence is 83%. Overall, the AML policies and procedures category has a 2.05 risk and 78.5% of firms on average experience low to high risk impact issues for this section. Overall, this is a slight reduction from 2016 which saw scores of 2.2 and 79%. High risk issues were found in 7% of cases.

Why is this? - There are always going to be record keeping issues to identify due to the volume of information that firms now process. Thankfully, which the reduced scoring reflects, and although occurrence is high, isn’t significant or systemic in nature and is reflected in a lower average score. Overall, a reduction is a step in the right direction, but considering that policies, procedures and record keeping are a product of training and internal procedures and not costly to enforce or control, it would have been beneficial to see a further reduction. Internal documentation as well as policies and procedures had the highest number of issues identified of any groups.
It is important to note that there is no alternative to record keeping as a risk-based approach. Firms must keep records of all documents used for CDD, any transactional records, and the data must be retained in the prescribed format as well as complying with Data Protection requirements.

A firm may state that they know their customers, and so do not need to keep adequate records. This is categorically incorrect, as record keeping is used for assisting investigations following SARs and thus rapid retrievability could be needed due to law enforcement requests, court orders, or visits by the regulators.

If the person who ‘knows’ the customer has left the firm or is on leave, how do firms with less than acceptable record keeping handle these requests? Training of staff is a vital tool for fostering a complete understanding of the importance of a seemingly tedious process, and a culture of compliance forms the foundation of consistent record keeping procedures.
Transaction monitoring remains a key hurdle for firms to get over. Alerts are generic and could be implemented better, we fully expect this to be a high priority for firms and regulators over the next few years.
CLOSING STATEMENT
BY PHILIP CREED

As financial crime reaches new levels of sophistication, financial services firms are striving to seek a fine balance between efficiency and effectiveness in order to prevent money laundering and terrorist financing. Financial services firms are using more advanced technologies such as AI, sophisticated data management and turning more and more to RegTech in their endeavour to provide efficiency savings in their approach.

Within this report, there is a general rise in standards in combating financial crime in the industry. Drivers include an increased scrutiny from both the regulator and banking providers as well as increased sophistication within the market itself, with better technology, better experienced staff and change in mindset. The majority of firms viewing compliance as a competitive advantage now as opposed to a necessary evil.

Money laundering is a global issue and the numbers are staggering.

- $2 trillion laundered funds currently in circulation
- $1.3 to $3.5 trillion annual cost of money laundering and associated crimes
- $12.4 billion total of the seven largest fines against banks for sanctions breaches
- $1 billion total average compliance investment for a global bank
- 70% increase in costs of compliance since the financial crash

Whilst several improvements have been made industry wide, there are key areas where I would expect to see further improvement next year. Transaction monitoring systems remain a problem. The majority of systems still cannot match KYC information to create bespoke monitoring rules based on that client. Too many systems use wholesale rules which are neither bespoke to the business nor the type of clients the business has. Many of these issues have come from a communication breakdown between compliance and technology teams. Several clients have employed a dedicated development team for compliance, a trend that is welcomed to combat the current skills gap between technology and compliance.

Training is often still viewed as a cost rather than as a competitive advantage. At fscom, experience has demonstrated that bespoke training delivered in house by the MLRO (where possible) is the most beneficial to the client.

Finally, I hope you enjoy the insights the report present. It is a cross section of the financial institutions that are clients of fscom and should not be interpreted as anything other than this. However, in producing such a document, it correlates with the challenges we see compliance officers encounter daily.

Kind regards,

Philip Creed
Director of Fincrime