A thematic review of trust and company service providers

May 2019

Executive summary

Background: trust and company services and money laundering risks

Money laundering is not a victimless crime. It is used to fund terrorists and facilitates drug dealers and people traffickers, as well as a range of other criminal activity. The credibility of solicitors and the services they offer makes them an attractive target for criminals, who want to launder their gains. Solicitors have a vital role - and opportunity - to help tackle the problem.

The creation and administration of trusts and companies on behalf of clients has been highlighted by the government as one of the legal service areas at highest risk of exploitation by criminals1 [#n1] . We agree with this assessment and it is reflected in our sectoral risk assessment. We have produced this document to set out information on money laundering and terrorist financing risks [/sra/how-we-work/reports/aml-risk-assessment/] that we consider relevant to those we supervise.

Trusts and companies are attractive to money launderers because individuals can:

- obscure the beneficial ownership and control of assets and wealth
- create and control multiple legal entities at a relatively low cost
- create complex and opaque structures
- operate across multiple jurisdictions
- avoid tax or duties.

They are the vehicle of choice for the legitimate investment and business world, however criminals may use them to add a veneer of legitimacy to illegal transactions.

The government is committed to disrupting and stopping money launderers and continuing to develop anti-money laundering (AML) and counter terrorist financing (CTF) requirements to monitor, assess and mitigate the risks posed by these vehicles2 [#n2] .

Our role

In July 2018, our Risk Outlook highlighted our growing concern about the risks and challenges posed to the profession by those looking to launder the proceeds of crime and finance terrorism. We explored this further in our Autumn update, where the concern was raised as a priority risk. Our interest in this area continues to intensify and is reflected in our significant, ongoing activities.

As a professional supervisory body, we have a statutory duty to make sure those we regulate assess risks and take proactive steps to mitigate and respond to money laundering issues. We must also take "effective, proportionate and dissuasive disciplinary measures3 [#n3] " where firms do not reach the required standard.

Our activities in this area are monitored by our supervisor, the Office for Professional Body Anti-Money Laundering Supervision (OPBAS).

What we did

In 2018 we reviewed 59 law firms in England and Wales that told us they carried out trust and company service provider (TCSP) work. We had initially planned to review 60, but upon visiting one firm we found they did not carry out this work. We met with firms, money laundering reporting officers (MLRO), money laundering compliance officers (MLCO) and fee earners.

At each firm, where possible, we reviewed two TCSP files. This report features findings from 115 file reviews.

We looked at each firm's compliance with the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017). The MLR 2017 place certain responsibilities on firms and individuals offering services most likely to be targeted by money launderers, including TCSPs. Around two thirds of the firms we regulate fall within scope of the MLR 2017.

This report summarises what we found. It builds on our two previous money laundering reviews in 2016 and 2017. These looked more generally at how law firms were tackling money laundering. The 2017 review also considered how they were responding to the government's money laundering regulations.

Headline summary

- In this review we found most law firms who carry out TCSP work are adequately meeting their obligations to tackle money laundering. Yet a significant minority are not doing enough, with some falling seriously short.
- We found no evidence of actual money laundering or that firms had any intention of becoming involved in criminal activities. Breaches of the MLR 2017 and poor training or processes could, however, mean firms are unwittingly assisting money launderers.
- Any AML system is an interdependent collection of policies and processes. Where one of these areas fails, it weakens the strength of the entire system. Areas where we had particular concerns included firm risk assessments, file risk assessments and the overall adequacy and availability of policies, controls and procedures.
- A firm risk assessment is required in legislation and should be the backbone of a firm's AML approach. We found that too many firms' approach was inadequate. More than a third of firms' (24) assessments did not cover areas required in legislation, this included a small number (four out of the 59 firms we visited) that had no risk assessment at all.
- Firms need to understand who their client is and what money laundering risks they pose. Our concerns in this area included inadequate processes to manage risks around politically exposed persons (PEPs) - an issue in around a quarter of firms. Some firms are also not doing ongoing customer due diligence (CDD), which is particularly important for TCSP work where the client can change. We did, however, find that 15 firms had turned down client instructions, with clients being evasive one of the main reasons.
- Most firms provided specific training about trust and company work and beneficial ownership. Poor training leads to poor compliance. Seven firms did not provide training on these topics and we have referred five of these into our disciplinary processes for breaches of the MLR 2017.
- Only ten firms - a sixth of our sample - had submitted suspicious activity reports (SARs) in the last two years. This tallies with concerns raised by the National Crime Agency (NCA) that generally law firms are not being proactive enough in looking to identify and then report suspicious activity.
- As a result of this review, we have referred 26 firms into our disciplinary processes. We will

judge each case on its facts and will be keen to see evidence that firms are moving swiftly to comply with their obligations. We will take strong action against firms where we have serious concerns that they could be enabling money laundering, and/or those who fail to address our concerns promptly.

- Other action we are taking includes:
  - publishing a warning notice highlighting our concerns, particularly in relation to firms' risk assessments
  - writing to 400 firms asking them to demonstrate compliance with the MLR 2017, focused on the approach to risk assessments
  - setting up a new dedicated AML team in the SRA, with increased resource to monitor and ensure compliance in this area.

Summary of findings by area

Most firms had appropriately assessed, monitored and mitigated the risks inherent within TCSP work. However, a significant minority of firms must improve across various areas.

Identifying and assessing risk

- Four firms failed to produce written firm risk assessments. This is a mandatory document and informs each organisation's controls and mitigations.
- Twenty-four firms had an inadequate file risk assessment that failed to cover various areas required by statute.
- Twenty firms were not able to show that they had specifically addressed TCSP work in their firm risk assessment
- Thirty-nine firms specifically covered TCSP work in their firm risk assessment.

Policies, controls and mitigation

- File reviews revealed 21 occasions where firms were unable to show they had continued to review CDD and keep it up-to-date.
- PEPs featured on six files we reviewed.
- We were only satisfied with 45 of the PEP processes we reviewed.
- We found no specific issues about the application of enhanced due diligence (EDD).
- AML training was provided at most firms but 17 firms failed to provide training about TCSP work. Of that 17, seven firms also failed to provide training about beneficial ownership.
- Firms had raised low numbers of internal suspicious activity reports (ISARs). These are reports about potential money laundering concerns raised by employees with the MLRO or deputy.
- Only 10 firms had submitted SARs in the last 24 months.
- Fifteen firms had turned down TCSP instructions for various reasons.

Open all [#]

Next steps

Disciplinary action following this review

Following our visits, we referred 26 firms into our disciplinary processes. We found no evidence of actual money laundering or that firms had any intention to be involved in criminal

activities. However, breaches of the MLR 2017 raise significant concerns about some firms' vulnerability to unwittingly assisting money launderers. These concerns are not isolated to any size or type of firm and we found issues across the profession.

The issues we have referred are statutory breaches of the MLR 2017. Where firms fall within scope of the MLR 2017, they must comply with the law. These requirements have been in place since June 2017. Even more worryingly some of the issues we found would have also breached the MLR 2017's predecessor, the Money Laundering Regulations 2007.

Money laundering poses a significant threat and where solicitors fail to take steps to mitigate this, we will always treat it as a serious issue and deal with it accordingly.

We are working closely with the 26 firms referred to our disciplinary processes to make sure appropriate changes are made to promptly reduce and mitigate the risks of money laundering. Where firms do not co-operate or the breaches are significant, we will consider disciplinary action. Our actions will reflect the seriousness of the breaches we have found and how firms respond.

Our wider enforcement work

Following this review, we have published a warning notice [/solicitors/guidance/compliance-money-laundering-regulations-firm-risk-assessment/] for solicitors and law firms to remind them of their duties in tackling money laundering, and in particular our concerns around firms' risk assessments.

We will take action where we find serious breaches of our rules. This is important to protect the public, uphold the rule of law, and maintain trust and confidence in the profession.

In the last five years, we have taken more than 60 cases, linked to potential improper money movements, to the Solicitors Disciplinary Tribunal. These cases have seen more than 40 solicitors being struck off, voluntarily coming off the roll, or suspended from practising.

At the beginning of May 2019, we had more than 160 live investigations into law firms linked to money laundering issues.

Monitoring compliance

We have a range of ways that we monitor AML risks in the sector and identify where there are compliance issues. This includes using artificial intelligence.

Following this review, we are carrying out more wide-reaching compliance checks. We recently wrote to an initial sample of 400 firms asking them to demonstrate compliance with the MLR 2017. We will be scrutinising the results over the summer with a view to undertaking further, similar exercises depending on our findings.

A dedicated AML team

Money laundering is a priority risk for us and the sector. Given the importance of our work in this area, we have created a specialised AML unit. By creating a dedicated team, our aim is to further improve our AML work - enabling us to effectively identify both emerging and established risks, and act as swiftly as possible when we see new risks emerging.

The newly created team will also continue to carry out further proactive, thematic reviews of key AML risks and areas.

Working together to tackle money laundering

We will continue to work with:

- key stakeholders and interested parties to develop our understanding of emerging money laundering risks and help the profession mitigate and understand the associated threats
- the NCA to support the improved use of SARs. We are focussed on making sure firms are submitting appropriate, timely and accurate reports.
- the profession, offering support to help them comply. This includes providing up-to-date information about current and emerging AML [/solicitors/resources/money-laundering/money-laundering/] risks through our sectoral risk assessment and risk outlook.

Introduction

Background

In March 2018, the international standards-setting body, the Financial Action Task Force (FATF) assessed the United Kingdom's AML and CTF system4 [#n4] .

In advance of the assessment, the government produced a national risk assessment (NRA). The risk assessment provides evidence and information about the money laundering risks posed to the UK economy. In 20175 [#n5] , the NRA highlighted:

"…companies and trusts (and similar structures) are known globally to be misused for money laundering. As a global financial centre, with individuals and businesses from all over the world choosing to invest and do business here, the UK is particularly exposed to criminal exploitation of otherwise legitimate economic activities and structures."

The NRA continued:

"…the services at highest risk of exploitation are trust and company formation, conveyancing and client account services. Solicitors may offer any or all of these services and are therefore at greatest risk."

Trust and company service provision is defined by the MLR 20176 [#n6] and broadly refers to any firm or individual whose business is to:

- form companies or other legal persons
- provide a registered office or business address for a company, partnership, other legal person or arrangement
- act or arrange for another person to act as a:
  - director or secretary of a company
  - partner (or in a similar position) for other legal persons
  - trustee of an express trust or similar legal arrangement
  - nominee shareholder for another person, unless the other person is a company listed on a regulated market which is subject to acceptable disclosure requirements.

We highlighted the risks associated with TCSP work during our first sectoral risk assessment in March 2018:

"Trusts or corporate structures which facilitate anonymity can help disguise the source or destination of money or assets. Law enforcement have flagged that many investigations of money laundering lead to opaque corporate structures, used to hide the beneficial owner of assets7 [#n7] ."

Significantly, TCSP work is not a discrete practice area and could occur whenever a trust or company is used within a transaction or arrangement. TCSP considerations could occur during a range of work including:

- mergers and acquisitions
- private client tax structuring
- probate
- conveyancing
- personal injury work.

To explore this risk further and learn more about TCSP work, we carried out a thematic project. Our findings are contained within this report.

Objectives

Our project aimed to:

- review and test each firm's AML practices, processes, systems and behaviours
- improve our understanding about the nature and extent of TCSP work
- identify common challenges firms face while implementing the MLR 2017
- raise awareness of best practice and ethical conduct
- challenge poor behaviours and practices and take appropriate action
- identify emerging or potential risks that may require us to carry out further analysis or mitigating actions.

Our statutory duties

As an AML supervisor, we must monitor the individuals we regulate and take necessary measures to secure compliance[8] [#n8] with the MLR 2017 for those firms that fall within scope. This report provides an overview of our proactive work.

We must also gather information about the firms we regulate[9] [#n9] under the MLR 2017 and, in particular, information about the number of individuals who carry out TCSP work[10] [#n10] .

Following the introduction of the MLR 2017, we are required to approve officers, managers and beneficial owners of the firms within scope of the regulations. In addition:

- new officers, managers and beneficial owners are required to apply to us for approval
- firms that provide TCSP services must have an AML supervisor and be registered with HM Revenue and Customs. We collect information about those we supervise and share it with HM Revenue and Customs who keep a record of firms wishing to carry out TCSP work.

In 2018, we collected this information through a profession-wide data collection exercise.

This report complements our continuing data collection and develops our understanding of TCSP work and the firms involved in this work.

What did we do?

During 2018, we reviewed 59 firms across England and Wales. We looked specifically at firms which offered TCSP services.

The visits included a discussion with the MLRO/MLCO about each firm's:

- identification and assessment of AML and TCSP risks

- general AML processes and procedures
- approach to TCSP work and how they mitigate the associated risks.

We then randomly selected a TCSP fee earner to assess the wider understanding of individuals at each firm. This included a review of two files involving TCSP work to check adherence to the firm's policies and procedures, their behaviour and overall AML compliance.

Points to note

- Our original sample included 60 firms who had informed us that they carry out TCSP work. However:
  - one of the firms we were scheduled to meet did not carry out TCSP work.
  - some firms only carry out occasional TCSP work. Two firms we visited were unable to provide two TCSP files. One could only provide a single file for review and the other had no appropriate files available.

  Therefore, when we provide a breakdown of the number of firms we found who were complying, this is out of a total of 59 firms.
- Our report contains data about 115 files we reviewed. The age of each matter limited the data we could collect. For example, we reviewed:
  - several files that were at an early stage so certain checks were in process or had not yet begun
  - some files did not feature source of funds and source of wealth checks because the work did not include the transfer of money.

Accordingly, data about the file reviews will vary.

Identifying and assessing risks

This section sets out how firms identify and assess the money laundering risks that their businesses face.

Why is it important?

Firms must identify and assess the money laundering risks that their businesses face. This is a fundamental part of the process and forms the cornerstone of any successful risk-based, AML regime. These risks may change and develop over time and firms must take steps to monitor the ongoing risks.

Firms must produce:

- a firm-wide risk assessment11 [#n11]
- a file risk assessment for each client/retainer12 [#n12] .

As a professional supervisory body, we must:

- monitor the individuals we regulate and take necessary measures to secure compliance13 [#n13]
- review the risk assessments carried out by firms14 [#n14] .

Findings

We looked at two specific areas:

- firm risk assessments
- file risk assessments.

Firm risk assessments

Firms are required to create a written risk assessment15 [#n15] and must be able to produce it to us on request16 [#n16] .

In creating a risk assessment, firms must consider the size and nature of their business17 [#n17] . They must also keep an up-to-date record in writing of all the steps they have taken18 [#n18] to produce the assessment. Ultimately, a firm must be able to provide us with "the information on which that risk assessment was based19 [#n19] ."

Four firms did not have a written firm risk assessment. This is a key document and informs an organisation's controls and mitigations. Three of these firms also had multiple offices. This exacerbates the problem and raises concerns about how standards and expectations are adequately set and communicated across the organisation.

The firm risk assessment must cover six risk factors20 [#n20] :

- areas identified by our sectoral risk assessment
- type of clients
- countries in which it operates
- its products or service areas
- types of transaction
- delivery methods.

Thirty-five firms provided a risk assessment that covered each of these areas. The remaining twenty-four risk assessments failed to cover various areas that are required by statute:

A failure to address these areas can heighten AML risks when combined with other factors. For example:

- two firms failed to consider the countries that they operate in and failed to have a PEP process in place
- two firms failed to consider the geographical location of their clients or the nature of their firm's work
- five firms failed to consider the types of transactions that they undertake. They also failed to provide information and procedures in their AML policy about scrutinising complex and/or unusual transaction or transactions that have no apparent economic or legal purpose
- one firm failed to address how they deliver legal services and also acknowledged that they do not see 5% of their clients.

A culmination of omissions and circumstances heightens a firm's vulnerability to money laundering. This underlines the significance of creating a holistic firm-wide risk assessment.

Firm risk assessments and TCSP work

Both the sectoral risk assessment and the NRA acknowledge that creating or managing trusts and companies is a high-risk activity. We stated:

"The sectoral risk assessment should form the basis for firms' own risk assessments along with the national risk assessment and a comprehensive knowledge of [their] services, clients and delivery channels.21 [#n21] "

We were interested to see how firms had incorporated the detail from our sectoral risk assessment into their own risk assessments.

Thirty-nine of the 59 firms undertaking TCSP work specifically covered TCSP work in their AML risk assessment. This suggests that firms have read the available guidance and assessed the acknowledged risks. In addition, some firms provided a specific risk rating for their TCSP activity:

We think this is a useful exercise and it helps to educate and influence other fee earners.

However, twenty firms22 [#n22] were not able to show they had specifically addressed TCSP work in their risk assessment23 [#n23] . Given that our sectoral risk assessment should inform each firm risk assessment, we query how TCSP work was adequately assessed by these firms.

File risk assessments

In addition to a firm wide risk assessment, firms must also produce file risk assessments for each file24 [#n24] . These risk assessments should reflect and reinforce each other. An effective firm wide risk assessment will help to meaningfully forecast issues that fee earners might encounter and policies address how they might avoid or mitigate emerging risks. Information gathered during file risk assessments will also help fine tune and develop the firm's risk assessment.

Of the 59 fee earners that we interviewed, forty five fee earners (76%) were able to provide a satisfactory response about risk assessments for each of their TCSP files. This suggests that some firms have adopted a system to help mitigate AML risks. We did however refer 14 firms for further investigation, comprising:

- five firms that did not have a file risk assessment process in place. This is concerning and suggests that some firms are not systematically addressing money laundering issues. This undermines the ability of fee earners to detect issues, report concerns and mitigate risks.
- nine firms that had a process in place, but the fee earner was unable to provide an adequate risk assessment for each file. These failures suggest some firms struggle to monitor the compliance levels of fee earners and/or fail to implement the process/policy.

Ongoing monitoring

Firms must continue to carry out ongoing monitoring of the risks once they have made an initial risk assessment about the client and transaction. Various aspects of the legal transaction may change including the:

- identity of the client
- circumstances of the client (they may become a PEP or alternatively cease to be a PEP)
- behaviour of the client (secretive)
- source of funds
- source of wealth
- legal instructions.

When these changes occur, the risk assessment and associated mitigation may also need to change.

Significantly, ongoing monitoring is not effective or possible where:

- firms/fee earners do not know what they are doing
- matters are not assessed at the outset
- risk assessments are not used or available for inspection by fee earners
- CDD is not completed or available for inspection by fee earners
- decisions are not recorded.

We asked firms about how they promoted ongoing monitoring:

Many firms used a combination of methods and this helps to strengthen their processes and overcome the inherent weaknesses of any single approach:

- Enshrining the significance and requirements of ongoing monitoring within processes and policies can be an effective way of ensuring fee earners understand and take appropriate steps. Introducing processes whereby files are audited and receive ongoing checks by separate teams is useful. Examples included checks being undertaken by the accounts team, compliance teams and team leaders. Forty-nine firms also had a policy in place to determine when CDD should be refreshed for returning clients. While this is useful, firms must still think about when to refresh CDD because an element of the transaction has changed. Regardless of the initial process/policy, firms must continue to monitor whether they are effective and produce the desired effect. Fee earners must also have access to the policy and understand it. Some of the methods we saw will not prevent money laundering and will only highlight an issue after it has occurred.
- Relying on fee earners to complete ongoing monitoring is an effective way to assign responsibility. A diligent fee earner can prevent money laundering issues before they occur. However, reliance is only effective when the fee earner has received appropriate training, understands what is required and has access to the relevant information. Firms must also have a system in place to check the fee earner is meeting the required standards.
- Physical systems can be used by firms to help carry out ongoing monitoring. Some firms had adopted e-verification systems to carry out CDD which continued to monitor each client and alert the fee earner/firm when the status of an individual changes. Other firms employed practice management systems that prompted fee earners to carry out ad-hoc checks about the client, the funds and the transaction. These systems can be effective when fee earners understand how to use the technology. However, this is not always the case and during two file reviews, we found evidence of PEP alerts not being investigated because the fee earners didn't understand the e-verification document.

File risk assessments are required by the MLR 2017 and firms are obliged to assess and monitor the risks posed by their clients and retainers. It is important that they are meaningfully carried out and monitored on an ongoing basis. The strength of a file risk assessment is dependent on the fee earner understanding the requirements and making an accurate assessment of the risks posed.

Policies, controls and mitigation

Why is it important?

Once firms have identified and assessed the money laundering risks they face, they must:

"…establish and maintain policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified in any risk assessment25 [#n25] ".

As an AML supervisor, we use a risk-based approach to check the adequacy of each firm's policies, controls and procedures to mitigate and manage effectively the risks of money laundering26 [#n26] . We must also seek compliance with the regulations27 [#n27] .

Findings

Policies and controls help each firm to mitigate and reduce the money laundering risks they face. Significantly, this can only be done if the firm has identified and assessed the money laundering risks they face. It is unlikely that a policy, process or mitigation will be adequate without the initial key assessment.

We looked specifically at:

- AML policies
- CDD
- PEPs
- EDD
- source of wealth and source of funds
- training
- lSARs and SARs.

AML policy

Firms must produce policies, controls and procedures to mitigate their exposure to money laundering risks28 [#n28] . These were often contained in a standalone AML policy but this is not a requirement.

Each policy must meet set requirements29 [#n29] . Policies should:

- be based on the risk assessment
- be approved by senior management
- be updated
- provide guidance about how to identify and scrutinise complex transactions
- provide guidance about how to identify transactions with no apparent economic or legal purpose
- be based on appropriate guidance.

Beyond the overarching issues around risk assessments, which would likely undermine a firm's policy and controls, we encountered various issues about the AML policies provided by firms:

- one firm had not updated their AML policy since 2007
- four firms did not have adequate guidance about how to identify and scrutinise complex

transactions. This issue is specifically highlighted in our sectoral risk assessment and the MLR 2017[30] [#n30]

- seven firms did not provide adequate guidance about how to identify matters that have no apparent economic or legal purpose. This issue is also specifically highlighted in our sectoral risk assessment and the MLR 2017[31] [#n31] .

We made eight referrals into our disciplinary processes about inadequate AML policies. This included one referral for a complete lack of written policies.

Customer Due Diligence (CDD)

A fundamental aspect of any successful AML system is the ability to understand who the customer is and what money laundering risks they pose.

Firms must carry out CDD whenever they establish a business relationship[32] [#n32] . Ultimately, this means the firm must identify and verify their client[33] [#n33] . This is a key part of assessing whether a client poses a money laundering risk.

CDD requirements will vary according to the type of client. When acting for a trust or company, the firm must obtain and verify the name of the organisation, a company/registration number and the registered office[34] [#n34] . There are also requirements to identify the control structure, all beneficial owners and take reasonable measures to verify their identity[35] [#n35] .

The importance of understanding beneficial ownership during TCSP work is highlighted in our sectoral risk assessment:

"Accurate and up-to-date information on beneficial owners is a key factor in preventing financial crime and tracing criminals who try to hide their identity behind corporate structures. Increased transparency reduces the risk of money laundering. Firms should be alert to customers seeking products or transactions that would facilitate anonymity and allow beneficial owners to remain hidden without a reasonable explanation."

We noted several issues during our file reviews:

- of the 59 firms we visited, the fee earner we spoke to at 10 of the firms (17%) was unable to provide the relevant CDD for each of their files
- eight files did not contain adequate information and/or recorded evidence about beneficial owners of the relevant trust or company
- one file featured a firm making payments to an apparent beneficiary without obtaining the obligatory ID.

A failure to gather CDD at the outset is a significant issue. It also undermines other AML safeguards and prevents firms from:

- carrying out ongoing monitoring
- assessing whether EDD is necessary
- accurately determining whether an individual is a PEP.

Identifying and verifying clients can be more difficult where firms are unable to meet TCSP clients in person. This is a risk that most firms will encounter at some point:

During our sectoral risk assessment, we acknowledged the risks that remote clients posed:

"Not meeting a client increases the risk of identity fraud and may help facilitate anonymity[36] [#n36] ."

Most firms acknowledged this and took steps to mitigate the risk:

- forty-nine firms had a process in place when dealing with clients they had not met
- ten firms refused to act for people that they had not personally met.

Ongoing monitoring

TCSP work can complicate CDD:

- managers, trustees, shareholders and beneficiaries may change. This is not unusual, and our file reviews noted 10 occasions where the client changed
- companies and trusts may be organised in structures
- structures can be complicated and opaque
- beneficial owners/controllers can take time to establish.

Accordingly, firms must monitor and refresh CDD on an ongoing basis[37] [#n37] to make sure the transaction is consistent with the individual's knowledge of the customer, their business and the risk profile[38] [#n38] . Individuals should also review existing records and keep the documents or information obtained for the purpose of CDD up-to-date[39] [#n39] . Forty-nine firms had a specific policy about when CDD must be refreshed. However, these policies usually focused on the lapse of time rather than a change in circumstances.

Our file reviews revealed 21 occasions where firms were unable to show they had continued to review CDD and keep it up-to-date. Although the CDD might have been accurate, it is unclear how firms reassured themselves of this. On one occasion, CDD had not been refreshed despite the identity of the client changing.

Firms should also consider whether their CDD process allows ongoing monitoring. During our file reviews we encountered three firms who stored CDD documentation in a central location. This unwittingly hampered (or excluded) fee earner access to the documents and prevented them from carrying out effective ongoing monitoring of CDD.

Politically exposed person (PEP)

A PEP is an individual who is or was entrusted with a prominent public function, their family or their close known associates. In general, they are considered to present a higher risk of potential involvement in bribery and corruption by virtue of their appointment. The appointment could be political or broader and includes:

- a member of the senior judiciary
- a high-ranking officer in the armed forces
- a senior figure in a state-owned enterprise
- a senior figure of an international body, such as the United Nations or an international sporting federation.

Firms must have appropriate systems and procedures to determine whether a client or a beneficial owner of a client is a PEP, or the family member or known close associate of a PEP[40] [#n40] .

To help determine what systems and procedures are appropriate, firms must consider several things including their firm risk assessment and the level of money laundering and terrorist financing inherent in its business[41] [#n41] .

Our sectoral risk assessment also highlighted PEPs as a high-risk:

"The 2017 Money Laundering Regulations updated the definition on PEPs so that individuals from the UK are now included, whereas previously the definition was restricted to overseas individuals. Generally speaking, PEPs have access to public funds and the money laundering regulations require PEPs and their close families and associates to be identified and require extra checks to mitigate the risks of corruption. The money laundering regulations require firms to be able to identify PEPs and associates, and to undertake enhanced due diligence on them42 [#n42] ."

During our file reviews we encountered six files that featured a PEP. This represents five percent of the files we reviewed and suggests this is not an unusual occurrence. With the broadened definition which now includes domestic PEPs43 [#n43] , firms are more likely to encounter PEPs or their family/associates during their day-to-day business.

When acting for a PEP a fee earner must44 [#n44] :

- have approval from senior management in order to continue the business relationship
- take adequate measures to establish the source of funds and source of wealth
- conduct enhanced ongoing monitoring of the business relation
- conduct EDD.

PEP Policy

A PEP policy helps to outline the firm's expectations and processes to fee earners. Although not explicitly required by the MLR 2017, a firm's policy and procedures are unlikely to be compliant without taking PEPs into account45 [#n45] . We found several issues about PEPs at firms:

- three firms did not understand what a PEP was. Accordingly, no checks were undertaken for any clients. This is a critical issue and suggests the firms are vulnerable to acting for PEPs without the relevant safeguards. This also raises queries about who the firm has unwittingly acted for in the past
- two firms had an out of date PEP policy that contained an inaccurate PEP definition. Both firms failed to consider domestic PEPs and this is not compliant with the MLR 2017.
- one file review featured a PEP but showed the firm's policy and process was not followed. This raises issues about the firm's ability to monitor compliance by fee earners and review the adequacy of the associated policies and processes.

These firms were referred into our disciplinary process unless they were able to remedy the issues promptly.

PEP system

Critically, firms must be able to identify PEPs. Having a process in place helps firms to identify individuals and take appropriate steps to mitigate the risk each PEP poses46 [#n46] . Reliance on a client to acknowledge they are a PEP does not address clients who may wish to conceal their identity. If a firm fails to have a PEP process in place, it naturally limits their ability to identify PEPs and mitigate the associated risks. Significantly, firms must be able to identify PEPs in order to meet other key requirements under the MLR 201747 [#n47] .

We were satisfied with 45 of the PEP processes that we reviewed. There is no required format for these systems and firms adopted various methods:

- forty-three firms used an electronic verification tool that carried out automatic checks

- five firms relied on a manual process for example internet searches
- twenty-one firms had a system that incorporated a two-stage check. This might include referring information automatically or manually to the MLRO, a compliance team or a managing partner for approval or further oversight.

However, we also encountered several issues:

- eight firms had no PEP process. These firms were referred into our disciplinary process.
- six firms had an inadequate PEP process:
  - four firms were reliant on clients to self-declare they were PEPs. Naturally, reliance on self-declarations is not an effective way to identify individuals who may be seeking to hide their personal history
  - two firms used an electronic system that only looked at foreign PEPs.

Firms were referred to our disciplinary processes where matters were considered significantly serious and firms were unable to promptly resolve the issue.

Enhanced Due Diligence (EDD)

EDD is required to manage and mitigate heightened money laundering risks. This may include (but is not limited to) where:

- the client is based in a high risk third country[48] [#n48]
- the client is a PEP (or a family member or known associate of a PEP)[49] [#n49]
- any other situation that presents a higher risk of money laundering or terrorist financing[50] [#n50]
- a transaction is complex and unusually large or there is an unusual pattern of transactions[51] [#n51]
- a transaction has no apparent economic or legal purpose[52] [#n52] .

We reviewed nine files that featured EDD. Firms had applied EDD for various appropriate reasons, including:

- six PEPs
- two overseas trusts/companies
- one client who was not seen in person.

Although we found no specific issues about the application of EDD, it is useful to remember the interrelated nature of any AML system. For example, if a firm does not have an appropriate mechanism to identify PEPs it will also weaken the firm's ability to detect when EDD is required. As mentioned, some firms failed to have an appropriate PEP system in place. We had similar concerns about other areas that will impact on a firm's ability to monitor and apply EDD.

Source of wealth & source of funds

TCSP work generates specific risks about understanding each client's source of wealth and source of funds. Our sectoral risk assessment acknowledges this:

"Trusts or corporate structures which facilitate anonymity can help disguise the source or destination of money or assets…Money launderers can seek to disguise the source of funds by having payments made by associates or third parties or have payments

made to third parties. This is a way of disguising assets and you should make sure you always identify the source of funds and source of wealth53 [#n53] ."

We asked firms about how they scrutinised source of funds and source of wealth. We were also interested about how and when ongoing checks were done throughout the life of the transaction. We found:

- thirty-four firms relied on fee earners
- twenty-three firms adopted a physical system
- two firms did not have a system in place.

Reliance on fee earners can be an adequate measure when the individual understands source of funds and wealth, the associated risks and how to respond when they occur. However, the file reviews showed this was not always the case:

- fifteen files did not feature adequate enquiries about the source of wealth
- fourteen files did not feature adequate enquiries about the source of funds.

A common problem was fee earners/firms were unable to differentiate between source of funds (where the money was coming from) and the source of wealth (how the money had been generated).

Numerous firms adopted a physical system that promoted checks and balances. A physical system requires action to be taken that can be checked and monitored by the firm. For example, providing information about the source of funds and wealth to a finance team in advance of any payment so the details are checked at the point of payment. This is useful because it means compliance is not reliant on an individual.

Training

AML compliance is a technical and nuanced area of regulation and firms must provide training for relevant employees54 [#n54] . Firms often told us that they relied on fee earners and staff to spot money laundering risks and issues. While this can work, firms must provide appropriate training and guidance.

We asked firms if they provided training about beneficial ownership and trust and company service provider work:

- fifty two firms provided training about beneficial ownership
- forty two firms provided training about trust and company work

This raises concerns about the limitations of some fee earners' knowledge and understanding.

Our visits highlighted seven firms who had not provided training on either topic. Significantly, five of these firms were subsequently referred for various breaches of the MLR 2017.

A lack of training is exacerbated when the MLRO also does not understand the position. This area is covered in more detail below.

Suspicious activity reports (SARs) and internal suspicious activity reports (ISARs)

TCSP work is an acknowledged high-risk area. We were interested about each firm's risk tolerance in this area. We looked at several areas including:

- ISARs made about TCSP work in the last 24 months
- SARs made about TCSP work in the last 24 months
- work turned away by firms.

We are unable to say whether firms/fee earners referred matters appropriately, but the limited volume of the referrals raised concerns:

We also asked firms about whether they had turned away TCSP clients. Fifteen firms had turned down instructions for a range of reasons:

The SAR regime is an integral part of the UK's AML and CTF system and solicitors have an important role to play. However, FATF recently commented:

"…there remains an underreporting of suspicious transactions by higher risk sectors such as trust and company service providers (TCSPs), lawyers, and accountants[55] [#n55] ."

Based on the firms we saw, we have real concerns about this area. As detailed above there is a huge variance in the volume of SARS and ISARs being submitted by firms. This variance is not always supported by the volume or nature of the work being carried out by those firms. The low level of ISARs suggests that there may be issues about the policies and procedures adopted by firms and/or the understanding of fee earners. Given the concerns raised by the NCA and FATF, this is an area that we will continue to scrutinise.

Money Laundering Reporting Officers (MLROs) and Money Laundering Compliance Officers (MLCOs)

Most firms should have an MLRO and MLCO (although there are a few narrow exemptions permitted in the MLR 2017). It is crucial that these individuals have appropriate training to help them make decisions and offer appropriate guidance to others. However, this was not always the case:

- Six MLROs told us that they had not received training. Significantly, four of these MLROs were at firms that were also referred into our disciplinary processes.
- We made three referrals which featured concerns about the ability and understanding of the MLRO.
- During one visit the MLRO was unaware that they were the MLCO until told by a colleague during the meeting.

Conclusion

Making sure the legal sector is tackling money laundering effectively is vitally important. The type of work law firms do, combined with the credibility of solicitors, make them an attractive target for criminals who want to launder proceeds of crime.

If we don't successfully address the problem, the social, economic and security consequences can be devastating. Doing all we can is also essential if we are to continue to maintain trust and confidence in the legal profession. That trust is vital to our country's continued success as a leading international centre for legal services.

Significantly, firms have a statutory duty to meet the requirements of the MLR 2017. These obligations have been in place since 26 June 2017.

Although most firms were able to show adequate systems, processes and procedures, we had concerns about a significant minority of firms. This is too many. Our concerns included issues about firm risk assessments, file risk assessments and the overall adequacy and availability of policies, controls and procedures.

Any AML system is an interdependent collection of policies, processes and procedures. Where one of these areas fails, it weakens the strength of the entire system. An inadequate AML system raises concerns about compliance and mitigation. However, it also raises concerns that firms might have unwittingly assisted money launderers in the past.

As set out in more detail in our Next Steps section [#headingOne] , following our visits we have referred 26 firms into our internal disciplinary process to further review their conduct.

Given the importance of this issue, we have also published a warning notice reminding the profession of their duties and particularly highlighting our concerns about firm-based risk assessments. We are also carrying out a further review of 400 firms' risk assessments.

We will continue our ongoing engagement with stakeholders to identify emerging risks and help the profession mitigate money laundering threats that arise.

AML continues to be a priority risk for us. We have created a dedicated team devoted to preventing and detecting money laundering, and this team will continue to build upon the work of this thematic review.

We will also continue to support firms by providing up-to-date, relevant information to help them tackle this problem, while taking action against firms that do not meet their ongoing AML obligations.

Notes

1. "National risk assessment of money laundering and terrorist financing" the National Risk Assessment, (2017)
2. For example, the introduction of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
3. Reg 49(d) MLR 2017
4. The FATF set standards and promote the effective implementation of measures to combat money laundering, terrorist financing and proliferation financing.
5. "National risk assessment of money laundering and terrorist financing" NRA (2017)
6. Reg 12(2) MLR 2017
7. www.sra.org.uk/sra/how-we-work/reports/aml-risk-assessment.page [/sra/how-we-work/reports/aml-risk-assessment/]
8. Reg 46(1) MLR 2017
9. Reg 51(1) MLR 2017
10. Schedule 4(3) MLR 2017
11. Reg 18 MLR 2017
12. Reg 28(12)(a)(i) and (ii) MLR 2017
13. Reg 46 MLR 2017
14. Reg 46(4)(a) MLR 2017
15. Reg 18(1) MLR 2017

16. Reg 18(6) MLR 2017
17. Reg 18(3) MLR 2017
18. Reg 18(4) MLR 2017
19. Reg 18(6) MLR 2017
20. Reg 18(2)(a) and (b) MLR 2017
21. www.sra.org.uk/sra/how-we-work/reports/aml-risk-assessment.page [/sra/how-we-work/reports/aml-risk-assessment/]
22. As mentioned above, one firm did not carry out TCSP work. Their data has not been provided.
23. Although 46 firms mentioned that they had incorporated our sectoral risk assessment
24. Reg 28(12)(a)(i) and (ii) MLR 2017
25. Reg 19(1) MLR 2017
26. Reg 46(4) MLR 2017
27. Reg 46(1) MLR 2017
28. Reg 19(1) MLR 2017
29. Reg 19 MLR 2017
30. Reg 19(4)(a)(i)(aa)
31. Reg 19(4)(a)(i)(bb)
32. Reg 27(1) MLR 2017
33. Reg 4 MLR 2017
34. Reg 28(3)(a) MLR 2017
35. Reg 28(3)(b) MLR 2017
36. www.sra.org.uk/sra/how-we-work/reports/aml-risk-assessment.page [/sra/how-we-work/reports/aml-risk-assessment/]
37. Reg 28(11)(b) MLR 2017
38. Reg 28(11)(a) MLR 2017
39. Reg 28(11)(b) MLR 2017
40. Reg 35(a) and(b) MLR 2017
41. Reg 35(2) MLR 2017
42. www.sra.org.uk/sra/how-we-work/reports/aml-risk-assessment.page [/sra/how-we-work/reports/aml-risk-assessment/]
43. Previously, PEPs only included overseas individuals but MLR 2017 has brought UK PEPs into scope
44. Reg 35(5) MLR 2017
45. Reg 19(4)(a)(ii) MLR 2017
46. Reg 35(1)(a) MLR 2017
47. Reg 33(1)(d) MLR 2017

48. Reg 33(1)(b) MLR 2017
49. Reg 33(1)(d) MLR 2017
50. Reg 33(6) MLR 2017
51. Reg 33(1)(f)(i) MLR 2017
52. Reg 33(1)(f)(ii) MLR 2017
53. www.sra.org.uk/sra/how-we-work/reports/aml-risk-assessment.page [/sra/how-we-work/reports/aml-risk-assessment/]
54. Reg 24(1) MLR 2017
55. "Anti-money laundering and counter-terrorist financing measures in the United Kingdom", FATF 2018