Solicitors Regulation Authority

Anti-Money Laundering (AML) Visits 2019-2020

November 2020

Contents

Executive summary

Background

We are a supervisory authority under The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("the regulations"). We have a role in checking firms are complying with the regulations and ensuring they have effective AML policies controls and procedures in place.

To help fulfil this, in 2019 we began an ongoing programme of firm reviews.

Our approach

We looked at the firms' approaches to preventing money laundering in 10 key areas. In each area we have outlined what the regulations say, our expectations, what we found, good practice and areas for improvement.

From September 2019 to October 2020, we visited 74 firms to review their AML policies and procedures and to see how these were being applied on a sample of the firm's files. We are grateful to the firms we visited for their time and insight into their work to prevent money laundering, particularly when the Covid-19 pandemic has disrupted work across the sector.

Key Findings

Overall, we found that the areas needing the most work from firms were:

- **Audit,** where some firms misunderstood the requirement for an independent audit and failed to test the effectiveness of their AML regime. More than half (38, 51%) required follow up action in this area. Of those, 14 firms (19%) had never conducted an audit.
- **Screening,** where firms were generally compliant with the requirement to screen employees on appointment, but 21% were failing to conduct ongoing checks.
- **Matter risk assessments**, which on 29% of files had not been carried out. This meant that the firms may have been unaware of high-risk matters passing through their hands.
- **Source of funds,** which had not been checked adequately or at all in 21% of matters. Failing to check a client's source of funds is likely to mean a failure to properly understand the risks involved in the transaction.

Further action

- Forty-seven (64%) required some form of engagement. This included requesting firms update their AML policies and reviewing revised versions to ensuring compliance. We also requested in some cases that firms agree a compliance plan to rectify any shortcomings, such as requiring a review of live files to ascertain the extent of a lack of customer due diligence. We then considered the results and provided recommendations to ensure compliance.
- Nine firms were referred to the AML Investigations Team for further investigation into whether there have been serious breaches of our rules, and any appropriate sanction.

Conclusion

The firms we saw were, for the most part, united in their determination to keep the proceeds of crime out of their client accounts, and we were able to assist many of them in meeting their obligations.

We saw a mixture of good and poor practices, but generally it was clear that in most practices there was a will to prevent money laundering and to comply with the regulations.

Audit was a particular matter of interest. While firms generally had an understanding that they needed to keep their policies, controls and procedures updated, a number of firms failed to monitor their effectiveness.

When reviewing firms' files, we found that in a large number there were differences between policies, procedures and what the money laundering compliance officer (MLCO) said should have happened, and what actually happened on the ground. This was often because the fee earners were not following procedures, something that could have been identified and rectified sooner if a compliant audit had been carried out.

Where we referred firms for further investigation, this was because what we saw suggested a systemic lack of compliance such as:

- at least 50% of the files reviewed showed serious issues, such as a lack of due diligence or matter risk assessments were not present
- a lack of an effective compliance framework, or indeed a lack of any AML policies, controls, and procedures at all
- an MLCO who did not appear to understand their obligations and was failing to carry out their role properly
- serious breaches by senior members of the firm, for example, one head of department who had failed to carry out sufficient AML checks on a politically exposed client from a sanctioned jurisdiction

This document should act as a guide to other firms on how they should approach the areas we now understand firms are unsure about.

Anti-money laundering (AML) visits 2019 – 2020

Introduction

Reducing the risk of law firms being involved in money laundering remains a priority for us and the profession. Firms continue to be an attractive target for criminals looking to launder criminal proceeds, as they provide legitimacy to transactions and handle large amounts of money.

Money laundering is not a victimless crime and is linked to the funding of terrorism and people trafficking. The vast majority of solicitors would be horrified to find they had unwittingly helped money launderers through ineffective policies and procedures.

What we did

As part of our role as a supervisor for AML, we visit firms to see if their systems are adequate and effective in preventing their firms from being used to launder money. This involves engaging with firms and performing spot checks of their compliance with the regulations, as well as discussing any other AML issues which may arise. From September 2019 we began a rolling programme of reviews. The firms we saw ranged in size, from a firm with three fee earners to the largest that had over 500. Over half had 50 or more fee earners. Geographically, 25 firms had their head offices in London and six in Wales, with the remainder spread across England. We will often prioritise higher risk firms for our proactive work, as a part of a risk-based approach, though we may visit firms at other risk levels also. This is the first report arising from this new programme.

Our visits involved testing firms' compliance with the regulations through meetings with:

- the firm's Money Laundering Compliance Officer (MLCO) and the firm's Money Laundering Reporting Officer (MLRO), to discuss their approach to AML and their overall internal policies and processes
- two fee earners, chosen on the day, together with a review of two of each of their files.

We adapted our methods twice during the period:

- The regulations were amended in January 2020, part-way through our visits, so we updated the questions we asked to take account of this.
- Due to the ongoing Covid-19 pandemic, from March 2020 we began conducting these reviews remotely.

We have set out our findings in ten key areas:

- Audit
- Due diligence
- Electronic verification
- Matter risk assessments
- Money Laundering Compliance Officers and their roles

- Sanctions
- Source of funds
- Staff screening
- Suspicious activity reports
- Training.

In each area we have outlined what we found, what the regulations say, our expectations and good and bad practice.

Next steps

We will continue to visit firms to check on compliance with the regulations and the adequacy and effectiveness of policies, procedures. Firms will need to be mindful, particularly in uncertain times that criminals continue to explore new ways of bypassing the checks and balances put in place to prevent money laundering. The risk may be currently heightened in that criminals will seek to exploit any weaknesses in firms as a result of Covid-19 and remote working.

During the course of our reviews, we worked with the firms to identify any regulatory breaches or shortcomings and to encourage best practice. Most firms required some form of action, even if generally the breaches we identified were minor and remediable.

Action with the firms

Of the firms we visited:

- Over half of firms (47) required some form of engagement and remedial action. The level of engagement depended on the action needed and included measures such as requiring:

    - amendments to a firm's AML policy and reviewing these to ensure compliance
    - specific corrective actions on files we reviewed
    - a formal review by the firm of all open files for AML compliance, with proposals for remedying any shortcomings or patterns of noncompliance found.

- 12 firms were issued with written guidance, but no formal follow up required.
- Nine firms were referred to the AML Investigations Team for further investigation and possible sanction.

That matters were referred does not mean that there had been a breach of our rules and that disciplinary action will follow.

Audits

What the regulations say

Regulation 21

(1) Where appropriate with regard to the size and nature of its business, a relevant person must:

(c) establish an independent audit function with the responsibility:
(i) to examine and evaluate the adequacy and effectiveness of the policies, controls and procedures adopted by the relevant person to comply with the requirements of these Regulations;
(ii) to make recommendations in relation to those policies, controls, and procedures; and
(iii) to monitor the relevant person's compliance with those recommendations.

What we found

- 18 firms reported both an internal and an external audit. Conversely, 14 had not conducted an audit at all.
- There was a tendency to assume that externally arranged audits were automatically compliant. On more than one occasion, we were handed a copy of an audit which, when examined, did not address AML compliance at all.
- 21 firms relied on accreditation schemes for an external audit, which generally did not address AML adequately or at all.
- 18 firms used other external providers, however not all addressed the effectiveness of their firm’s policies, controls, and procedures.
- 41 firms told us that they had conducted an internal audit of some kind. However, these were not always compliant with Regulation 21.
- Four firms said they were unaware of the requirement to have an independent audit.
- The independence of an auditor can be an issue. The job of conducting an internal audit was often given to MLRO/MLCO or compliance department. This was problematic because they were then assessing the adequacy and effectiveness of their own work.
- Both external and internal audits ranged from an update of policies and procedures which would not amount to an audit, to very comprehensive reviews of policies and files, fee earner interviews and annual reports.

- In many instances improvement and compliance was a simple case of adjusting firms' existing measures, for example policy updates or file reviews, and applying independent oversight.

What we expect

We consider that Regulation 21 should be interpreted as follows:

- **Size:** Only at the very smallest practices will a Regulation 21 audit not be appropriate to the firm's size. All other practices who carry out regulated work must establish an audit function.

- **Nature:** We expect most firms to carry out an internal audit. If firms consider they do not need to carry out an audit, they will need to justify this based on their size and nature. We consider that the following are some indicators that a firm is of a nature that requires an audit:
    - Having more than one office.
    - Having fee earners who focus on an area of regulated work e.g. conveyancers.
    - The partners being responsible for others' compliance with the regulations.

- **Independent:** This does not necessarily mean engaging a specialist agency or consultancy, though that is an option. Firms should make sure that, as a minimum, those with responsibility for maintaining their AML framework are not those auditing it. As well as an external entity, this could for example be:
    - a senior member of the firm who does not carry out regulated work
    - an MLRO from another firm
    - an office manager with no regulatory or fee-earning role
    - a reciprocal arrangement between small firms to review each other's compliance

- **Adequacy:** The audit must check whether the firm's policies, controls and procedures are:
    - up to date with the law, regulations and regulatory guidance
    - suitable for the work the firm carries out
    - appropriate to the firm's size and nature.

- **Effectiveness**: The audit should consider whether the firm's policies, controls and procedures are being followed and are serving their intended purpose. This is difficult to evidence without a review of files.

- **Make and monitor recommendations:** The auditor must be of sufficient seniority to police this and make sure that any recommended measures are put in place. If an external provider is used, the recommendations should become the responsibility of a suitably senior and independent person within the firm.

- **Regularity:** The regulations do not specify a time period for audit. We would suggest an audit:
    - of policies, controls, and procedures when the regulations change
    - following revision of the firm's policies, controls and procedures
    - following any other major change at the firm (for example a merger with another firm)
    - at a regular interval determined by the size and nature of the firm, for some an annual basis may be appropriate

- In many cases, we found that the file reviews we undertook did not reflect the firm's policies and procedures. Time and effort spent drafting and implementing policies might prove to be wasted if fee earners are unaware of them or ignore them. We suggest that a compliant audit, including file reviews, is likely to be the best way to make sure that policies are being followed.

- Where firms engage an external agency to conduct an audit, it is for them to ensure that it meets the requirements of Regulation 21. The responsibility to produce a compliant audit remains with the firm and cannot be transferred.

Good practice	Areas for improvement
• At one firm, the auditor had explicit authority to bypass the managing director. This was a measure which was intended to ensure their independence. • Another firm included interviews with new starters as part of their audit. • One firm conducted AML file reviews on both an annual and an ad hoc basis.	• Several firms carried out a simple update of policies, controls, and procedures, without any attempt to consider their effectiveness. • A lack of independence: the MLRO/MLCO, for example, may and should contribute to the audit but it should be overseen by an independent party. • Failing to keep written records of previous audits. • Failing to implement recommendations in a timely way.

Due diligence

What the regulations say

Client, or customer, due diligence (CDD) is governed by Regulations 27 and 28. It sets out measures which must be applied to clients in the regulated sector. These are basic measures for establishing a client's risk level, identifying them and verifying their identity.

Simplified due diligence (SDD) is a process by which, under certain low risk circumstances, firms may apply a less rigorous standard of customer due diligence. It is governed by Regulation 37.

Reliance is where a firm wholly relies on due diligence carried out by another party, and is governed by Regulation 39. If firms wish to do this, they must meet certain obligations. The responsibility to make sure sufficient customer due diligence was conducted still rests with the firm.

Politically exposed persons (PEPs) are a class of client who hold prominent public office and pose a high-risk of money laundering. Regulation 35 sets out firms' obligations when taking on PEPs as clients, which include enhanced due diligence. The same obligations apply to any clients who are family members or known associates of PEPs.

What we found

- On 39 (53%) matters, insufficient CDD had been collected. This was deficient for several reasons, including:
    - The client being known to one of the firm's partners – this was not, however, noted on the file and they were not known to the file holder.
    - An expired paper driving licence counterpart was produced, with no other supporting information.
    - CDD collected on only one of several joint clients.
    - The CDD 'probably' being on another file, which could not now be found.
    - The fee earner assuming that the central compliance team had gathered it.
    - The CDD not being accessible to the fee earner who held the file.
- 47 firms (64%) said they did not use SDD, even though in many cases the policy provided for it. It was variously seen as too vague, risky, or confusing.

- Only six firms (8%) relied on due diligence provided by others under r39. In these cases, it was generally used for overseas clients or where the client referral came from a regulated person.

- Only eight (11%) firms had no written policy on (PEPs). Of those, however, six firms had a process in place to identify PEPs.

- To identify PEPs:

    - eight firms relied on a declaration signed by the client
    - 41 firms relied solely on e-verification
    - ten firms used both methods.

- 67 firms (91%) had turned away a potential client because of the AML risks they posed. Several firms said that they had not explicitly turned the client away but had simply imposed enhanced due diligence requirements in line with the risk posed, and the client had ceased to contact them.

- In 15 cases, Enhanced Due Diligence (EDD) should have been undertaken but had not been. In one of these cases, the client was an Iranian PEP dealing with a number of offshore jurisdictions. Despite this, the firm's own notes on the case explicitly stated that EDD was not required.

- In 20 cases, insufficient due diligence had been gathered to make the assessment as to whether EDD was required.

What we expect

- Those collecting CDD should be aware that the requirement is to identify and verify the client, and that passports, driving licences and utility bills are only one way of doing this. If a client cannot produce documents such as these, there are other ways of identifying and verifying them.

- Many firms use a centralised compliance team to collect CDD information. We have no objection to this but consider that as a minimum the fee earner holding the matter must understand this information and have access to it. Once a matter has begun, we consider the fee earner holding the file is best placed to conduct ongoing monitoring and assess ongoing risk.

- Compliant audits, as set out above, will be of assistance in making sure that:
    - matters are properly risk assessed
    - CDD is carried out on all relevant parties to a suitable standard
    - source of funds and wealth checks are carried out where appropriate.

- There is no set way to identify PEPs, nor is there a central list. PEP status may be lost and gained rapidly and is more widely defined than many firms assume. Both client declarations and e-verification are valid ways of identifying a PEP,

but both have risks and limitations of which firms should be aware. For example:

- e-verification is likely to be most useful in identifying high-profile PEPs, but less likely to identify their family members and associates
- client declarations are only useful if the client is honest with the firm and is aware that they are a PEP (as many may not be).

We would suggest that a combination of different methods is likely to offer the firm the most security.

- It is for firms to decide their own risk appetite, but their policies should be realistic. With the proper policies, controls and procedures, there is nothing to prevent a firm taking on PEP clients. If a firm has an overly restrictive PEP policy, it is at risk of:
  - turning away clients for no good reason restricting access to legal services
  - being counter-productive if the firm has a policy which is ignored or routinely breached.

- Under regulation 35, firms must conduct "enhanced ongoing monitoring" of PEP clients. The wording indicates that the ongoing monitoring must be of a higher standard than for other clients of the firm. As a minimum, we would expect firms to:
  - keep a written record of any PEP clients
  - arrange regular meetings with the MLCO/MLRO and fee earners dealing with PEP files to monitor progress.

- Where a firm has decided against using SDD or reliance, this should be clear from the policy. We would expect this to be picked up in a regulation 21 audit as part of checking the policy's adequacy.

Good practice	Areas for improvement
• A creative approach to CDD when conventional documents are not available. • Storing due diligence centrally and accessibly so that it can be used for multiple client matters and will not be inaccessible when a matter is closed. • Systems preventing billing until CDD is completed.	• Fee earners being unable to access CDD and other information, making ongoing monitoring difficult if not impossible. • A stereotypical view of PEPs as wealthy and high-profile individuals. • Outdated definition of PEPs as overseas figures only. This definition was changed in 2017. • An assumption that PEPs would not instruct the firm.

• Using more than one method to identify PEPs. • Keeping in regular touch with fee earners dealing with PEP clients. • Appreciating the risks posed by simplified due diligence and reliance and exercising appropriate caution.	• Including provisions in the firm's policies, controls and procedures for activities which are barred in practice.

Electronic verification

What the regulations say

Regulation 28

(19) For the purposes of this regulation, information may be regarded as obtained from a reliable source which is independent of the person whose identity is being verified where—

(a) it is obtained by means of an electronic identification process, including by using electronic identification means or by using a trust service (within the meanings of those terms in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23rd July 2014 on electronic identification and trust services for electronic transactions in the internal market F12); and

(b) that process is secure from fraud and misuse and capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact the person with that identity.

What we found

- Electronic verification (e-verification) is the use of third-party systems to verify clients. Typically, a firm using such a system will enter a client's details. These details will then be used to search various databases (eg the sanctions database) and open-source checks (eg Companies House) and adverse media checks.
- Most of the firms we spoke to (63 firms or 85%) used an e-verification system. This was divided among 25 different providers.
- 11 firms used more than one e-verifier, with some using as many as three. The systems are different and some are better at dealing with different types of client.
- The suitability of some of the systems used is questionable, however. One, used by two firms, appeared to be a search system for determining property title which did not establish client identity or verification.
- Five firms said they only used e-verification for some of their clients:
  - two said only for conveyancing clients
  - one said only used at one of the firm's several offices
  - one said only for individuals
  - one said only on an ad hoc basis.

What we expect

- There is nothing in the regulations which mandates the use of e-verification.

  Firms may wish to consider how they can use other means to fulfil the due diligence requirements of the regulations, in particular:

  Regulation 27
  Regulation 28
  Regulation 33
  Regulation 35.

  This is particularly important in relation to sanctions and PEP checks.

- Firms remain responsible for their AML compliance. Use of an e-verification service alone will not be sufficient to ensure a compliant system. Often, the e-verification system explicitly flags issues for further investigation.

- Firms should check that their e-verification service is suitable for their client profile.

- Firms should periodically test their e-verification systems against known figures (eg members of the firm or prominent public figures) to check its accuracy.

- In most cases, e-verification alone is unlikely to satisfy the requirements of the regulations. While most systems are likely to be able to identify the client insofar as a person of that name exists, additional steps may be needed to verify the client is who they say they are as required under regulation 28(2).

Good practice	Areas for improvement
• A holistic approach to due diligence which uses e-verification as a check on certain aspects of a client's profile, together with other checks. • Taking care to guard against user error when submitting client information. A passport, for example, is a simple way of ensuring that a client's name is spelt correctly. • One firm noted that ISIS terrorists had been made subject to	• Using e-verification on an ad hoc occasional basis, rather than a risk basis. • Over-reliance on e-verification to cater for all a firm's due diligence needs. • Manually overriding, or manipulating the score to achieve a pass, without using the tool properly. • Lack of training which can lead to user error

sanctions. They tested their e-verifier to see whether it was up to date. It was not, so they changed provider.	

Matter risk assessments

What the regulations say

Regulation 28

(11) The relevant person must conduct ongoing monitoring of a business relationship, including:

(a) 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;

(b) undertaking reviews of existing records and keeping the documents or information obtained for the purpose of applying customer due diligence measures up to date.

(12) The ways in which a relevant person complies with the requirement to take customer due diligence measures, and the extent of the measures taken:

(a) must reflect:
the risk assessment carried out by the relevant person under regulation 18(1);
its assessment of the level of risk arising in any particular case;
(b) may differ from case to case.

(13) In assessing the level of risk in a particular case, the relevant person must take account of factors including, among other things:

(a) the purpose of an account, transaction or business relationship;

(b) the level of assets to be deposited by a customer or the size of the transactions undertaken by the customer;

(c) the regularity and duration of the business relationship.

Regulation 33

(6) When assessing whether there is a high risk of money laundering or terrorist financing in a particular situation, and the extent of the measures which should be taken to manage and mitigate that risk, relevant persons must take account of risk factors including, among other things:

(a) customer risk factors, including whether:
(i) the business relationship is conducted in unusual circumstances;
(ii) the customer is resident in a geographical area of high risk (see sub-paragraph (c));

(iii) the customer is a legal person or legal arrangement that is a vehicle for holding personal assets;
(iv) the customer is a company that has nominee shareholders or shares in bearer form;
(v) the customer is a business that is cash intensive;
(vi) the corporate structure of the customer is unusual or excessively complex given the nature of the company's business;
(vii) the customer is the beneficiary of a life insurance policy;
(viii) the customer is a third country national who is applying for residence rights in or citizenship of an EEA state in exchange for transfers of capital, purchase of a property, government bonds or investment in corporate entities in that EEA state;

(b) product, service, transaction or delivery channel risk factors…, including whether—
(i) the product involves private banking;
(ii) the product or transaction is one which might favour anonymity;
(iii) the situation involves non-face-to-face business relationships or transactions, without certain safeguards, such as an electronic identification process which meets the conditions set out in regulation 28(19);
(iv) payments will be received from unknown or unassociated third parties;
(v) new products and new business practices are involved, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products;
(vi) the service involves the provision of nominee directors, nominee shareholders or shadow directors, or the formation of companies in a third country;
(vii) there is a transaction related to oil, arms, precious metals, tobacco products, cultural artefacts, ivory or other items related to protected species, or other items of archaeological, historical, cultural or religious significance or of rare scientific value;

(c) geographical risk factors, including:
(i) countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to counter money laundering or terrorist financing;
(ii) countries identified by credible sources as having significant levels of corruption or other criminal activity, such as terrorism (within the meaning of section 1 of the Terrorism Act 2000 **F10**), money laundering, and the production and supply of illicit drugs;
(iii) countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;
(iv) countries providing funding or support for terrorism;
(v) countries that have organisations operating within their territory which have been designated:
(aa) by the government of the United Kingdom as proscribed organisations under Schedule 2 to the Terrorism Act 2000, or
(bb) by other countries, international organisations or the European Union as terrorist organisations;
(vi) countries identified by credible sources, such as evaluations, detailed assessment reports or published follow-up reports published by the Financial Action Task Force, the International Monetary Fund, the World Bank, the Organisation for Economic Co-operation and Development or

other international bodies or non-governmental organisations as not implementing requirements to counter money laundering and terrorist financing that are consistent with the recommendations published by the Financial Action Task Force in February 2012 and updated in June 2019.

(7) In making the assessment referred to in paragraph (6), relevant persons must bear in mind that the presence of one or more risk factors may not always indicate that there is a high risk of money laundering or terrorist financing in a particular situation.

What we found

- In 86 of the 294 files we reviewed (29%), there was no written matter risk assessment. In various matters:
  - an analysis had been carried out, but there was no conclusion as to the file's risk level, making it difficult for the firm to know if EDD should have been carried out
  - the clients were personal friends of the fee earner or a partner in the firm – relevant to the risk level, certainly, but not a reason not to assess
  - the risk assessment amounted to simply asking whether the client was a PEP or not
  - the fee earner wrongly assumed that the firm's e-verification system did this for them.

- Even if a matter was risk assessed, on some occasions this conflicted with the firm-wide risk assessment. One firm-wide risk assessment, for example, stated that all conveyancing matters should be considered high-risk and EDD should be carried out. When we examined two conveyancing files, both were stated to be low-risk and EDD had not been completed.

What we expect

- Firms should make sure that their fee earners understand the need to carry out matter risk assessments. They should also be aware of the circumstances set out in the regulations that require EDD and would therefore be considered high risk.
- Matter risk assessments must, under regulation 12(12)(a), reflect the firm-wide risk assessment. Those assessing client and matter risk should have access to the firm-wide risk assessment and be encouraged to consult it.

Good practice	Areas for improvement
• Making risk assessment an integral part of opening a client file.	• Carrying out a risk assessment and failing to record it.

• The consequence of the assessment is clear in terms of when enhanced due diligence is required, and what measures that may include.
 	
• Some firms had set up files so that they cannot be worked on or billing recorded unless the matter has been risk assessed.
 	
• Requiring the matter risk assessment to be reviewed at certain milestone points such as file opening, exchange and completion.
 	
• Setting out factors which the fee earner needs to consider.
 	
• Standard form risk assessments can be helpful in:
  ○ reducing the time taken to assess matter risk
  ○ standardising the firm's risk assessment procedures
  ○ evidencing that an assessment has taken place.
	• Matter risk assessments which conflict with the firm-wide risk assessment.
	
	• Matter risk assessments containing lists of factors that made a matter high risk which did not sufficiently take account of the regulations.
	
	• Pro-forma risk assessments which due to their layout, or lack of corresponding guidance, did not prompt a proper risk assessment.

MLCOs and their roles

What the regulations say

Regulation 21

(1) Where appropriate with regard to the size and nature of its business, a relevant person must:

> (a) appoint one individual who is a member of the board of directors (or if there is no board, of its equivalent management body) or of its senior management as the officer responsible for the relevant person's compliance with these regulations;

What we found

- All the firms we visited had an MLCO appointed or were in the process of changing the role-holder.
- At 57 firms (76%), the MLCO and MLRO were the same person.
- Regarding screening, eight MLCOs expressed some uncertainty as to the measures the firm carried out. In some cases, they appeared to consider this not to be part of their role.
- 10 MLCOs and 10 MLROs had not received training geared to their own responsibilities. In eight of these cases, both roles were held by the same person.
- From our discussions it appeared that some MLCOs did not fully understand their overarching responsibility for compliance and were not engaged in the process.

What we expect

- We will be conducting a thematic review into the roles of MLCOs and MLROs in 2021 which among other matters will consider what training and experience might be appropriate for those holding these roles and what makes a good MLRO/MLCO. In the meantime, we refer to the LSAG Guidance 3.4.2:

> *Appointing an individual as the officer responsible for the practice's compliance with the regulations.*

The individual must be either a member of the board of directors (or equivalent management body) or senior management. A member of senior management means an officer or employee with sufficient knowledge of your practice's money laundering and terrorist financing risk exposure and sufficient authority to take decisions affecting that risk exposure.

The requirement to appoint an officer responsible for compliance with the regulations is additional to the requirement to appoint an MLRO. However, your practice's officer responsible for compliance with the regulations may also be your MLRO or, if applicable, your Compliance Officer for Legal Practice, provided they are of sufficient seniority.

- Except in the case of sole practices with no staff, we expect all firms to nominate an MLCO. It is important to have a nominated person responsible for ensuring compliance with the regulations.
- We expect the MLCO to be our main point of contact with us on any AML matter, and to take a leading role in dealing with us.
- Firms must use Form FA10B to notify us of a new MLCO or MLRO appointment.
- MLCOs should be aware of the breadth of their responsibilities under regulation 21. This includes, among other things:
    - screening
    - training
    - audit
    - the compliance of the MLRO with their own obligations under the regulations and the Proceeds of Crime Act 2002 (POCA), if the two role-holders are different people.

  The MLCO is not required to have direct involvement in all of the firm's relevant processes and procedures but must retain oversight of them. However, they must understand the issues and take their role seriously.
- The MLCO's compliance obligations involve co-operating with us on AML-related matters. We have referred one MLCO for further investigation because he was failing to respond to requests for information.

Good practice	Areas for improvement
• Where the MLRO and MLCO are different people, working well together to make sure that the firm's AML framework is effective. • Adopting a holistic approach to AML which embraces various	• Seeing the MLCO's role as primarily concerned with compliance activities such as collecting due diligence, rather than oversight and assurance.

functions such as recruitment and training. • Appointing a proactive and empowered MLCO who can hold fellow senior managers to account.	• Complete abdication of the MLCO's duties to the MLRO, who is not accountable for overall compliance. • Overloading the MLCO with different roles, leaving them with insufficient time and capacity to fulfil their duties under the regulations.

Sanctions

What the regulations say

Regulation 33

(6) When assessing whether there is a high-risk of money laundering or terrorist financing in a particular situation, and the extent of the measures which should be taken to manage and mitigate that risk, relevant persons must take account of risk factors including, among other things:

(c) geographical risk factors, including:
(iii) countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;

What we found

- 57(77%) firms ran sanctions checks on all new clients. Of these firms, 39 also ran checks on existing clients.
- Seven firms never checked clients for sanctions. Where reasons for this were given, they tended to assume that sanctioned individuals would not instruct the firm.
- Four only checked conveyancing clients for sanctions.
- One firm changed e-verifier for failing to pick up recent additions to HMT's sanctions register.

What we expect

Firms should make sure that they do not act for sanctioned individuals or businesses without a licence from HM Treasury.

It is dangerous for firms to assume that sanctioned individuals would not seek to use their firm. As at 12 August 2020, 47 individuals on the sanctions register were British nationals. The rise of supranational, non-state terrorist groups such as ISIS means that it is now more difficult to gauge who may or may not be sanctioned.

Most e-verification systems include a sanction check as standard. Alternatively, firms can themselves check HM Treasury's sanctions register online here.

Good practice	Areas for improvement
• A firm noticed that several sanctioned ISIS members originated from their own town. They checked their client list for these people. • The same firm noticed that their e-verification provider had not updated their database to include sanctions against ISIS members. As a result of this, they changed provider.	• Assuming that sanctioned individuals would not instruct the practice. The same assumption often also applies to PEPs. • Seeing sanctions checks as a one-time activity when new clients are taken on, with no regard to ongoing monitoring.

Source of funds

What the regulations say

Regulation 28(11)

(11) The relevant person must conduct ongoing monitoring of a business relationship, including:

(a) 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;

(b) undertaking reviews of existing records and keeping the documents or information obtained for the purpose of applying customer due diligence measures up to date.

(12) The ways in which a relevant person complies with the requirement to take customer due diligence measures, and the extent of the measures taken:

(a) must reflect:

(i) the risk assessment carried out by the relevant person under regulation 18(1);
(ii) its assessment of the level of risk arising in any particular case;

(b) may differ from case to case.

(13) In assessing the level of risk in a particular case, the relevant person must take account of factors including, among other things:

(a) the purpose of an account, transaction or business relationship;

(b) the level of assets to be deposited by a customer or the size of the transactions undertaken by the customer;

(c) the regularity and duration of the business relationship.

What we found

- 63 of the 294 files we reviewed (21%) did not evidence the client's source of funds properly or at all. In a few cases, there was a legitimate reason for this such as the matter having stalled. In others, however, the fee earner did not understand the requirement or made assumptions about the client's means. This last point particularly appeared when the client was known to one of the firm's partners.

- A few firms said that they would not always obtain information on the source of funds until comparatively late on in the transaction. For example, the information might only be completed just before exchange in conveyancing files.

- In corporate transactions, some fee earners felt that the firm's published accounts, obtained from Companies House, evidenced the client's source of funds. These accounts, however, are invariably drawn up one year in arrears. Or in some cases were not showing sufficiently available funds for the transaction.

- Several firms provided clients with a source of funds form with their client care documents. This provided a useful basis for fee earners to know what requests to make of the clients and what sort of questions might need to be asked.

- In one case, a fee earner had obtained client bank statements but had simply filed them without reading them.

What we expect

- Firms are required to check source of funds where necessary, under regulation 28(11). We consider however that carrying out and evidencing a source of funds check is also crucial in order to comply with its other obligations

    - For example, a solicitor could not be said to have properly assessed the risk of the matter under regulations 28(12) and (13) or determined whether EDD is necessary under Regulations 33(1) and (6), without evidencing the source of funds.
    - This is not limited to transactional matters – for example, a solicitor instructed to set up a trust would need the source of the settlor's funds to properly assess the risk.

- We consider that it is best practice to obtain evidence of the client's source of funds early in a transaction, for the following reasons:
    - If the source of funds causes concerns sufficient for a suspicious activity report to be sent to the National Crime Agency, this is likely to be far more disruptive, and cause delay, at critical stages in the transaction than if the information is gathered early on.
    - The source of funds should be an integral part of the matter risk assessment, so it makes sense to establish this at the outset.

- Firms should also consider whether, without making enquiries and evidencing a client's source of funds fully, they can be certain that they are not facilitating money laundering under s.327 of the Proceeds of Crime Act 2002.

Good practice	Areas for improvement
• Applying the same standards to all clients, regardless of any personal knowledge. • Gathering as much evidence as is needed to be sure of the source of funds. • Managing client expectations of the process by setting out what information will be required at the outset of the retainer.	• Assumptions about a client's source of funds and wealth based on anecdotes and perceptions rather than evidence. • Gathering source of funds evidence, such as bank statements, but failing to review it.

Staff screening

What the regulations say

Regulation 21

(1) Where appropriate with regard to the size and nature of its business, a relevant person must:

(b) carry out screening of relevant employees appointed by the relevant person, both before the appointment is made and during the course of the appointment;

(2) For the purposes of paragraph (1)(b):

(a) “screening” means an assessment of:
(i)the skills, knowledge, and expertise of the individual to carry out their functions effectively;
(ii)the conduct and integrity of the individual;

(b) a relevant employee is an employee whose work is:
(i) relevant to the relevant person's compliance with any requirement in these regulations, or
(ii) otherwise capable of contributing to the:
(aa) identification or mitigation of the risks of money laundering and terrorist financing to which the relevant person's business is subject, or
(bb) prevention or detection of money laundering and terrorist financing in relation to the relevant person's business.

What we found

- Firms generally have a good grasp of screening on employment, but less so on regular checks once employed.
- Firms generally were not aware of what ‘screening’ means under the regulations, there was a widespread assumption that it meant Disclosure and Barring Service (DBS) checks.
- Nine MLCOs expressed some degree of uncertainty about pre/post-employment checks, for example, assuming that Human Resources had carried out checks but being uncertain as to what.

Pre-employment – 72 firms (97%) carried out some form of check.

- The most basic was checking with the us or the Law Society whether person is a solicitor.
- The most comprehensive checks involved qualifications, references, regulatory history, and DBS, 36 firms carried out all four.
- 15 firms carried out checks (most commonly DBS checks) only on certain staff, to meet the requirements of the Conveyancing Quality Scheme.
- Other measures included: passport/driving licence checks, running the person's name through the firm's e-verification, credit checks, social media checks.

In-employment checks – 58 firms (78%) carried out some form of check.

- 65 firms (88%) did not carry out any regulatory checks on fee earners once employed.
- 28 firms (38%) mentioned appraisals, which can be an effective way of screening for both knowledge and integrity. The actual total may be higher as many firms did not initially consider this to be screening.
- 13 firms limited ongoing checks to the minimum required to qualify for the Conveyancing Quality Scheme. This meant that ongoing checks were limited to property and finance staff only.
- 12 firms (16%) placed reliance on annual self-declarations.

What we expect

1. On appointment

a. Skills, knowledge, and expertise:
- Qualification checks (seeing original certificates)
- Validating practising status via the Solicitors Register or applicable regulator

b. Conduct and integrity:
- Taking up references
- Checking disciplinary history via the Solicitors Register or applicable regulator
- Adverse media checks via search engines.
- E-verification, if available

2. During employment (annually)

a. Skills, knowledge, and expertise

- Annual competence declaration
- Appraisal procedure

b. Conduct and integrity

- Adverse checks via search engines.
- Checking disciplinary history via the Solicitors Register or applicable regulator or emailing. contactcentre@sra.org.uk
- E-verification, if available.

Firms will also need to consider, as part of their risk-based approach, whether it is necessary to undertake DBS checks on any relevant employees, and if so, how frequently these should be refreshed. They should also consider, for example, whether their beneficial owners, officers and managers under the regulations require credit checks.

Asking fee earners to self-certify annually that they have not been convicted or cautioned for any criminal offence, or subject to regulatory sanction, is not on its own likely to be an effective method of screening. The Solicitors Disciplinary Tribunal case of SRA v Podger (12065-2020) is an example of a solicitor failing to declare a drugs conviction to both his firm and to us.

Firms who limit their in-employment checks to those required by the Conveyancing Quality Scheme are in danger of positioning money laundering as an issue which only affects conveyancing. These checks do, of course, go towards addressing a very high-risk area for money laundering, and are certainly better than nothing. Firms should, however, be aware that the regulations govern activities, not practice areas. See Regulation 11(d) and Regulation 12 for more information.

Good practice	Areas for improvement
• Using multiple methods of screening to ensure that a firm knows as much about its fee earners as possible. • Seeing screening as an ongoing process, not a one-time check at the point of employment.	• Reliance on fee earner declarations alone. MLCOs should consider the risk posed to the firm should a false or incorrect declaration be made. • MLCOs' unfamiliarity with screening processes is a risk for them and their firms. MLCOs have the responsibility of maintaining the firm's compliance with the regulations, which includes screening.

• Relying on independent sources, rather than personal knowledge of the fee earner. • Adopting a holistic approach to screening, embracing existing measures such as annual appraisals, and checking referees.	• Firms limiting screening to conveyancing staff, in accordance with accreditation schemes, may also pose a risk. Conveyancing is a high-risk area for money laundering, but it is not the only one. • Reliance on personal knowledge of a person before they commence employment with the firm, with no independent checks.

Suspicious activity reports (SARs)

What the law and regulations say

Proceeds of Crime Act 2002 (POCA 2002), Part 7

Those within scope of the regulations must make a SAR (called a disclosure in the legislation) if, as part of the course of their business:

- they know or suspect that another person is engaged in money laundering
- they have reasonable grounds to know or suspect that another person is engaged in money laundering
- they know the identity of the person engaged in money laundering, or
- that they believe, or it is reasonable to expect them to believe, that the information which gave rise to the knowledge or suspicion will or may assist in identifying that other person or the whereabouts of any of the laundered property.

Regulation 21

(3) An individual in the relevant person's firm must be appointed as a [MLRO].

(4) A relevant person must, within 14 days of the appointment, inform its supervisory authority of:

(b) the identity of the individual first appointed under paragraph (3); and
(c) of any subsequent appointment to either of those positions.

(5) Where a disclosure is made to the [MLRO], that officer must consider it in the light of any relevant information which is available to the relevant person and determine whether it gives rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion that a person is engaged in money laundering or terrorist financing.

What we found

- We asked firms how many times, in the previous 24 months:
  - staff had made an internal suspicious activity report (iSAR) to the MLRO
  - the MLRO had made a suspicious activity report (SAR) to the National Crime Agency.

- In the preceding 24 months:
  - 16 MLROs received **0 iSARs**
  - 32 MLROs received **1 to 10 iSARs**
  - 19 MLROs received **11 to 49 iSARs**
  - seven MLROs received **more than 50 iSARs** (the highest single total was 412).

- The wide spread of results is likely to be due to the variety of ways firms interpret iSARs. Some record every query made of the MLRO an iSAR, while others only record expressions of concrete concern about a client.

- In the preceding 24 months:
  - 25 firms had submitted **0 SARs**
  - 43 firms had submitted **1 to 10 SARs**
  - Six firms had submitted **11 to 50 SARs** (50 was the highest number).

- Most fee earners we spoke to correctly understood that if they developed knowledge or suspicion of money laundering, it should be reported to the MLRO. Some, however, said they would discuss the matter with their supervising partner, head of department, or head of compliance in the first instance.

What we expect

- Firms should make sure that all staff know how to make a report to the MLRO and when this should be done.

- There is nothing wrong with discussing a potential report with a partner or head of department rather than the MLRO in the first instance, and in many ways, this is to be encouraged. It may be that they have a better insight into the client or the matter. However, if you still have suspicions, you should still speak with your MLRO. Staff should understand that a report to the MLRO is the only way to ensure their position is protected if their suspicions turn out to be correct, under s.330(4)(a) POCA 2002.

- Firms should foster a culture where staff feel able, and are able, to contact the MLRO if they have any AML concerns about a matter. They should feel able to err on the side of caution and be supported in making reports, and to keep the MLRO updated on individual matters.

- Firms which require iSARs to be made in a specific form should consider whether this might put people off reporting. An initial, informal, conversation with the MLRO can help to decide which matters should go forward to a formal internal report and which are simply queries about case and client handling.

- Maintaining records of any iSARs will not only help MLROs identify any risks, trends, and patterns the firm may be facing, but may also be used as a defence to criminal proceedings. Further information on keeping a record of suspicions and disclosures can be found in the LSAG AML Guidance.

This is a complex area, and considerations about legal professional privilege may also be relevant. For further information, see the LSAG Guidance, pp.87-106.

The importance of SARs

Some MLCOs expressed frustration with the SAR reporting process, among other things commenting that they did not understand what reports were used for or whether the information they provided was ever used.

The extract below is a real case study which the National Crime Agency's Financial Intelligence Unit (UKFIU) experienced. This shows that all information which is reported is potentially valuable, no matter how insignificant it may seem.

> *A foreign national became a victim of modern slavery after being duped via a romance scam to travel to London. She managed to use her controller's phone to call the police in her country. She informed them that she believed she was being held in South London and provided details of the 'boyfriend' of the romance scam. The overseas authorities contacted their police attaché who immediately called the Modern Slavery Unit within the Metropolitan Police Service (MPS). The detective used Arena to search the Elmer database and identified a potential match for the 'boyfriend' within payment details of a SAR relating to a different male suspected of being linked to modern slavery, due to spending patterns matching red flag indicators previously shared with reporters by the UKFIU.*
>
> *The officer identified and contacted the financial institution of the 'boyfriend', who were able to provide a potential new address for him. Within two hours of the victim notifying her national police, MPS officers were able to attend this new address and safeguard the victim. It further transpired that the victim was due to be moved to another address that evening and that only the 'fast time' support of the reporter meant that the MPS was able to safeguard the victim.*
>
> Extracted from *SARs in Action*, Issue 3 November 2019

The person who reported the red flags in this case will, in all likelihood, never know of how important their SAR was. The victim of this case, however, owes her freedom and likely her life to their vigilance.

Good practice	Areas for improvement
• Staff knowing who the MLRO is and how to make a report. • Appointing a deputy MLRO (or multiple deputies) to provide cover when the MLRO is unavailable or indisposed. • A visible and approachable MLRO who staff know they can turn to when in doubt. • Using examples of iSARs and SARs in training, to demonstrate good practice. Producing annual reports of iSARs and SARs, for inclusion in the firm's regulation 21 audit.	• Processes and procedures which make submitting an iSAR a time-consuming or daunting process. • Failing to keep records of iSARs, meaning that the MLRO cannot follow emerging patterns.

Training

What the regulations say

Regulation 24

(1) A relevant person must:

(a) take appropriate measures to ensure that its relevant employees, and any agents it uses for the purposes of its business whose work is of a kind mentioned in paragraph (2), are:

(i) made aware of the law relating to money laundering and terrorist financing, and to the requirements of data protection, which are relevant to the implementation of these regulations; and

(ii) regularly given training in how to recognise and deal with transactions and other activities or situations which may be related to money laundering or terrorist financing;

(b) maintain a record in writing of the measures taken under sub-paragraph (a), and in particular, of the training given to its relevant employees and to any agents it uses for the purposes of its business whose work is of a kind mentioned in paragraph (2).

(2) For the purposes of paragraph (1), a relevant employee is an employee whose work is:

(a) relevant to the relevant person's compliance with any requirement in these regulations, or

(b) otherwise capable of contributing to the:

(i) identification or mitigation of the risk of money laundering and terrorist financing to which the relevant person's business is subject; or

(ii) prevention or detection of money laundering and terrorist financing in relation to the relevant person's business.

(3) In determining what measures are appropriate under paragraph (1), a relevant person:

(a) must take account of:

(i) the nature of its business;

(ii) its size;

(iii) the nature and extent of the risks of money laundering and terrorist financing to which its business is subject; and

(b) may take into account any guidance which has been:

(i) issued by the FCA; or

(ii) issued by any other supervisory authority or appropriate body and approved by the Treasury.

What we found

- We were encouraged to see that 63 firms (85%) had provided firm-wide AML training within the past year.
- Only four firms had never provided any firm-wide training, and of those, three had provided some form of training to key fee earners. The remaining firm was relatively new and planned to conduct training shortly.
- 55 firms (74%) used more than one method of training. Of the remainder, 13 firms used e-learning alone, three used internal training alone, and one used an external provider alone. We would expect the popularity of e-learning to increase due to the ongoing pandemic.
- In terms of the popularity of training methods:
    - 62 firms (84%) used e-learning such as webinars or online courses
    - 42 firms (57%) used internal training provided by someone from the firm
    - 8 firms (11%) engaged an external expert to train staff.
- In terms of non-fee-earning staff:
    - 60 firms (81%) gave AML training to receptionists
    - 64 firms (86%) gave AML training to administrative staff
    - 69 firms (93%) gave AML training to finance staff.
- We were very encouraged to see that some firms had made sure to assess how non-fee-earning staff could play a part in preventing money laundering:
    - Three firms had emphasised that reception staff played a key role in their AML framework, given that they see clients in unguarded moments. One MLRO said that receptionists had often reported concerns to him.
    - Another firm provided AML training to delivery drivers and warehouse workers. While the firm understood that they were unlikely to come across money laundering in their work, it could not be ruled out, so they had training appropriate to their particular role.

What we expect

- The definition of ‘relevant employee’ in regulation 24(2) is very wide and firms should interpret it as such. We do not consider that it refers to fee earning staff alone, and other staff can play a key role in assisting in the identification, mitigation, prevention, or detection of the risk of money laundering. For example:
    - administrative staff will often be responsible for gathering and collating due diligence, and their work may involve building a rapport with the client

- reception staff see clients in unguarded moments, and will need to know how to deal with any cash offered by clients
- finance staff will need to know how to recognise suspicious payments into the firm's accounts and how to deal with unexpected transactions.

- The regulations do not specify a timescale in which training should take place, other than that it should be undertaken 'regularly'. We suggest that:
  - training should be provided on a regular basis, perhaps annually
  - provided to new starters as soon as practicable
  - provided on any changes to the regulations and associated legislation or regulations.

- Training should, where possible, be provided to staff in a way that is relevant to their own role in the firm. Generic training geared to fee earners is unlikely to be wholly relevant to administrative staff or receptionists. Likewise, staff in different practice areas are likely to face different risks. A detailed firm-wide risk assessment will be of assistance here.

Good practice	Areas for improvement
• Tailored training for staff in different roles and practice areas. • Creative thinking about how to involve non-fee-earning staff in the firm's AML framework. • Using more than one method of training. • Using training methods which test staff knowledge. • Notifying staff of examples of important AML developments, both within the firm and externally.	• Failing to maintain training records, and therefore being unable to tell who has or has not been trained. • Infrequent training, which allows AML knowledge to become stale and out of date. • A hands-off approach to training from the MLCO.