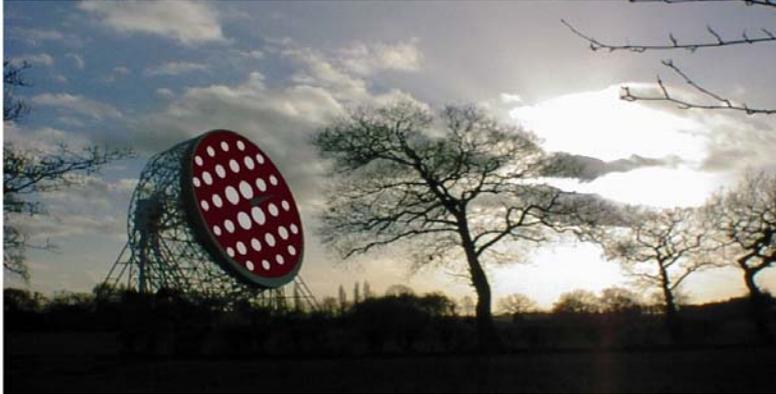


Risk Update • September 2020



The SRA are reviewing law firms' AML compliance remotely

In this Issue

- Anti-money laundering (AML)
- Risk and Audit Committees
- Professional indemnity insurance (PII)
- Data protection and information security

Note

This newsletter is a general guide. It is not a substitute for professional advice which takes account of your specific circumstances and any changes in the law and practice.

Subjects covered change constantly and develop.

No responsibility can be accepted by the firm or the author for any loss occasioned by any person acting or refraining from acting on the basis of this.

Anti-money laundering (AML)

Coronavirus has not prevented the Solicitors Regulation Authority (SRA) from continuing its review of law firms, in a number of cases auditing remotely. Nor has it changed firms' obligations under The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR).

It follows, that if firms have, out of necessity or practicality, adapted their compliance procedures, for example by conducting verification by video conferencing such as Zoom or Teams, or using biometrics, a risk-based approach is still required, and notes of deliberations, reasoning and decisions on the firm's approach must be kept. The SRA has published a coronavirus update covering *Help with common compliance queries*, which includes a section on *Client Due Diligence and ID checks* and we mentioned the Legal Sector Affinity Group (LSAG) Advisory Note: *COVID-19 –and preventing Money Laundering/Terrorist Financing in Legal Practices* in our May 2020 Risk Update.

The SRA has also been active in prosecuting those who breach the MLR, and two cases in the Solicitors Disciplinary Tribunal (12071.2020 and 12084-2020) have identified issues which apply to firms of all sizes.

The need for appropriate Customer Due Diligence (CDD) was emphasised: in one case, the respondent did not obtain certified copies of identity documents, and did not obtain complete identity documents from all the directors; a driving licence appeared to show tape marks to the left of the digits and the passport photo was not central to the photo box, with the neck of the person in the photo going outside the bottom of the box, and the person in the photo not appearing to have any shoulders. In the other case, a document had been signed by an unnamed notary in the Isle of Nevis.

The agreed outcome in one case noted that the MLR require 'ongoing monitoring of a business relationship' (see regulation 28 (11)) and 'scrutiny' to ensure that the transactions are consistent with the source of funds and nature of transactions in the context of the customer's business and risk-profile. The agreed outcome in each of these cases noted –

'The word 'scrutiny' is important to underline. The Regulations do not require a superficial check or even an averagely comprehensive check, rather they require scrutiny – which implies a critical, probing examination or exploration and it is submitted clearly places importance on the level of ongoing monitoring expected.'

Other breaches identified include failure to have a firmwide risk assessment, failure to train staff, failure to identify clients as Politically Exposed Persons (PEPs), failure to apply enhanced CDD measures and enhanced ongoing monitoring to PEPs, and failure to maintain adequate client records.

We have audited many of the larger UK and US firms under regulation 21 of the MLR, including remote audit. Even those firms which may strictly not require an external audit may wish to consider how they can prepare for an SRA visit. The SRA has proposed visits to all firms which they perceive as high-risk on a three-year rolling basis, along with visiting a sample of lower risk firms.

Fraud continues to be a significant concern. The Law Society has issued an updated *Practice Note on Property and Registration Fraud*, and the SRA has published a thematic review entitled *Investment Schemes That Are Potentially Dubious*.

Our News page, www.legalrisk.co.uk/News, contains links to the guidance referred to above, and to recent HMRC guidance for Trust and Company Service Providers (TCSPs) in carrying out risk assessments, the HM Treasury AML and CTF Supervision report 2018-19, JMLSG guidance on pooled client accounts and the latest Basel AML Index ranking money laundering and terrorist financing risks around the world. Further materials are on www.legalrisk.co.uk/AML.

Risk and Audit Committees

For larger firms with risk and/or audit committees, our News page www.legalrisk.co.uk/News includes links to *Terms Of Reference For The Risk Committee* published by the Chartered Governance Institute and a *Guide For Audit And Risk Committees On Financial Reporting And Management During Covid-19* published by the National Audit Office.

Professional indemnity insurance (PII)

Many firms will be experiencing a more expensive renewal of their PII, with more probing questions from insurers than before, including analysis of how firms have dealt with restrictions and conditions arising from coronavirus. We have produced two webinars in conjunction with Howden insurance brokers, and links are on www.legalrisk.co.uk/News. These address emerging claims and compliance risks from the current economic conditions and the PII renewal.

We have advised many firms with renewal issues on block notifications to help them ensure as far as practicable that claims arising from problem cases are covered under the current year's policy.

We are also seeing an ever greater number of policy coverage disputes, particularly in relation to multiple related claims such as hotel, student let and other investment schemes.

Firms which decide to close down should see the SRA's recent guidance on *Firm closure due to financial difficulties* and case studies. A link appears on www.legalrisk.co.uk/News.

Data protection and information security

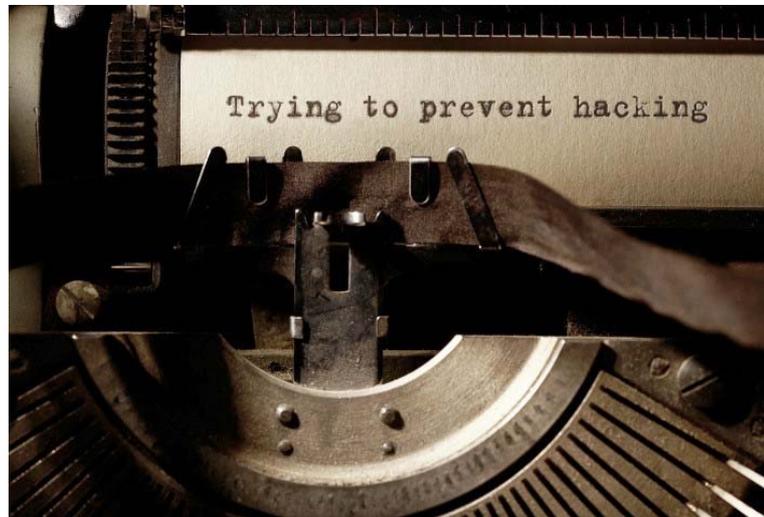
The decision of the Court of Justice of the European Union in in Case C-311/18, *Data Protection Commissioner v Facebook Ireland and Maximilian Schrems*, invalidating the use of the Privacy Shield for international data transfers to the United States, has attracted much publicity. (Links to the decision and other extensive data protection resources are on www.legalrisk.co.uk/Data.) However, in our experience, most (but not all) American and other law firms with US offices rely on the standard contractual clauses.

However, these too face challenges in the light of the decision. They cannot simply sign a contract containing standard contractual clauses and leave a copy in the bottom drawer. They also need to bear in mind the need, emphasised in paragraph 133 of the Schrems II decision, for assessment of measures in relation to data transferred to the US, and indeed other jurisdictions where the protection of privacy rights may fall short of those in the EU, particularly, for example, Hong Kong.

The European Data Protection Board has published Frequently Asked Questions on the decision. A link can be found on www.legalrisk.co.uk/News.

Meanwhile, we await revised EU standard contractual clauses, updated guidance from the Information Commissioner's Office, and, of course, news of what steps will need to be taken following the expiry of the transition period under the UK Withdrawal Agreement which maintains the UK's pre-Brexit arrangements until 31 December 2020.

A link to *The Sedona Conference Commentary on Law Firm Data Security*, which includes model clauses for engagement letters and a sample law firm information security questionnaire, can be found on www.legalrisk.co.uk/News.



Russia's security agency, the FSO, was reported to have bought typewriters to prevent leaks