





## Client Alert

November 2016

[Download](#)

| [Forward](#)

| [Contact Us](#)

| [Visit Our Website](#)



### Financial Crime Checklist

On 21 November 2016 the FCA issued a booklet aimed at consumer credit firms setting out good and bad practice on compliance with obligations under the Money Laundering Regulations 2007 (**MLR**). While directed at consumer credit firms, the booklet is, of course, relevant to all firms subject to the MLR.

#### **AML Focus**

Financial crime is one of seven regulatory priorities for the FCA according to its 2016/17 Business Plan. It also remains an area of enforcement focus with the FCA. Most recently, on 12 October 2016, the FCA fined Sonali Bank £3.25m for a series of money laundering systems and controls failings. The Bank's MLRO was also fined and prohibited from holding the MLRO function and from performing any MLRO or compliance oversight function.

#### **Risks**

The risks posed to consumer credit firms differ from risks for other financial services firms. According to the JMLSG, in the consumer finance context the main money laundering risk arises from an acceleration in the repayment schedule whereby the borrower may seek to use

tainted funds to repay borrowings and launder money in that way. Lenders also have to deal with fraud and identity theft issues which can also feed into money laundering concerns.

## The Checklist

We set out below the key messages from the FCA together with recommendations on action that firms should take.

Subject	Requirement	Action
Risk Assessment	Carry out a risk assessment proportionate to the nature and scale of your activities.	<p>The carrying out of risk assessments should be a continuous process. The suggestion in the FCA booklet is that too often these are regarded as one-off or annual exercises. However, firms need to conduct a regular review of risks.</p> <p>Adequate resources should be focussed on areas of risk identified.</p>
Policies and procedures	Effective, up to date and accessible policies and procedures should be prepared.	Policies and procedures should be reviewed and kept up to date. The practical application of policies and procedures should be reviewed/audited regularly to ensure that they are appropriately applied and implemented. This should also highlight whether changes should be made to existing policies and procedures.
Governance	Senior management must be fully engaged in oversight of financial crime matters and must be aware of the financial crime risks to which the firm is subject. They should also set the right tone from the top.	<p>Firms should ensure that senior management responsibility for financial crime risks is appropriately documented. This assists in demonstrating clarity around the allocation of responsibilities and assists in evidencing compliance.</p> <p>Tone from the top can be a cliché. However, active "hands on" involvement by senior managers in dealing with financial crime issues will show that the issue is taken seriously across the organisation.</p> <p>Senior management should receive management information on financial crime risks, including the output of risk assessments. Senior management involvement in financial crime issues should be documented, for example, through board minutes or minutes of other compliance committees or forums.</p>
Staff Awareness	Relevant financial crime training must be provided to staff in key roles.	Monitoring and HR processes should ensure that staff compliance with financial crime requirements and processes is reviewed and any

		deficiencies addressed. The FCA cite as an example of good practice the monitoring of employees' work to ensure that they have an understanding of risks relating to the firm.
Data Security	Firms must have written data security policies and appropriate systems and controls in place to ensure customer data is kept safe.	Data security must not be treated as exclusively an IT or privacy issue, but financial crime risks must also be taken into account. Access to data should be limited to those who require access in order to perform their roles. From a governance perspective responsibility for data security should be allocated clearly. Beware when outsourcing that appropriate controls are put in place.
Anti-Money Laundering (AML)	Where firms are subject to the Money Laundering Regulations they must establish and maintain systems and controls to reduce the risk that the may be used to handle the proceeds of crime.	AML procedures should be risk based so that the same customer due diligence (CDD) procedures should not be applied across all customers and products.
Enhanced Due Diligence (EDD)	Where there is a higher risk of money laundering, from certain clients such as PEPs or higher risk jurisdictions, firms must undertake EDD.	Senior managers should be involved in approving higher risk customers and be aware of what additional checks are required.
Ongoing monitoring / Suspicious Activity Reporting	Firms must conduct on-going monitoring of their business relationships on a risk-sensitive basis.	Firms should draw on the information they have about their customers and their activities with a view to detecting unusual or suspicious behaviour.
Record-keeping	The FCA requires retention of customer identity records for five years <u>after</u> the business relationship.	Make sure that your firm's policies and procedures reflect this requirement. Practically, it is also important that this information can be retrieved quickly and easily for compliance staff and also should the regulator ask to see it. Where reliance is placed on third parties make sure that they have adequate procedures as your business remains responsible.

Of all the above issues, there are two in respect of which firms should place special emphasis.

### **Governance**

Governance: the accountability of senior managers to guard against financial crime is provided for under high level standards in the FCA Handbook in respect of systems and controls. In this regard, a firm must allocate to a director or senior manager (e.g. the money laundering reporting officer) overall responsibility. It is vital that proper reporting lines are in place and that information can reach management and relevant committees in a timely fashion

for consideration and action, where necessary. With the roll out of the Senior Managers and Certified Persons Regime to all financial services firms in 2018, the incentive on managers to ensure that reasonable steps have been taken will be further increased.



### **Data Security**

There is also the threat posed by cyber attacks and the corresponding need to ensure data security. The growing use of technology in delivering services to clients, the sheer amount of data and its nature makes cyber security a key issue. The Data Protection Act 1998 requires that information must be kept securely and protected against criminals who would, for instance, commit identity theft. Good data security policies and appropriate systems and controls are a necessity in ensuring that staff understand their responsibilities and in demonstrating compliance to regulators, including the Information Commission's office with their growing penalty powers.

### **Contacts**


For more information and to discuss any of the issues arising from the implementation of 4MLD please contact Arun Srivastava ([arun.srivastava@bakermckenzie.com](mailto:arun.srivastava@bakermckenzie.com)) or Richard Powell ([richard.powell@bakermckenzie.com](mailto:richard.powell@bakermckenzie.com)).

### **For more information:**

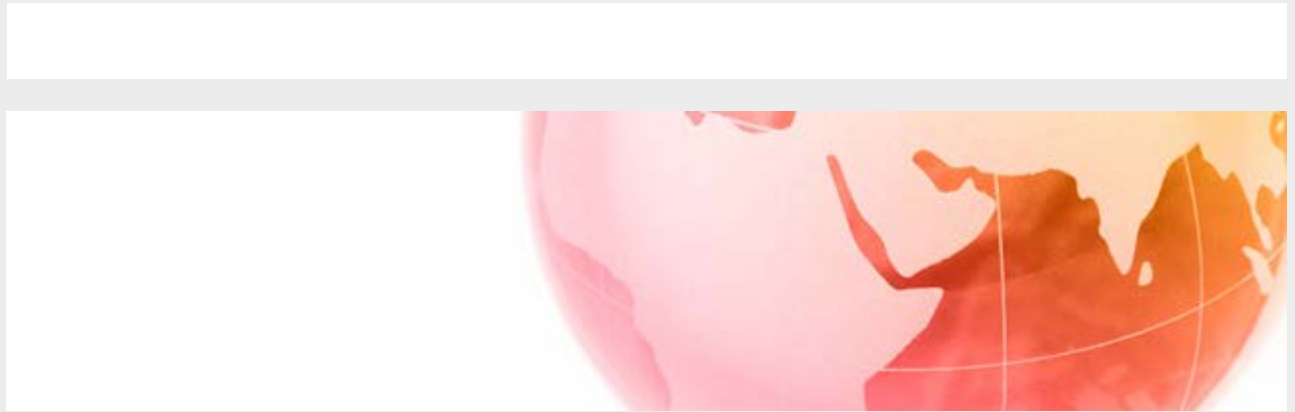


#### **Arun Srivastava**

Partner

+44 20 7919 1285 

[arun.srivastava@bakermckenzie.com](mailto:arun.srivastava@bakermckenzie.com)



Disclaimer - Baker & McKenzie International is a Swiss Verein with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm.

This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.