RIAA Barker Gillette

September 2016

CallCredit Fraud Summit 2016: The Future of Digital Identity

Steven Barker

AML in the Regulated Sector: A Quick Guide

Knowing the legal framework

Regulated businesses and nominated compliance and reporting officers employed therein are regarded by politicians and law enforcement agents as gatekeepers. We are required and expected to know the statutory and regulatory regime governing our obligations and what is required of us.

For those of us working in the regulated sectors, our Anti Money Laundering (and Terrorist Financing) obligations can be ascertained from the following legislation and regulations, namely:

- the Terrorism Act 2000;
- Part 7 of The Proceeds of Crime Act 2002 (**POCA**);
- the Money Laundering Regulations 2007; and
- various obligations arising out of international treaty and conventions, not the least of which are EU AML Directives. We are currently working with the third European Directive. The fourth has been enacted; more of which later.

All of the above have been amended to varying degrees by subsequent legislation and it is easy to find online up-to-date legislation and regulations incorporating the current source material with amendments. See for example www.legislation.gov.uk.

Although this presentation deals with AML, I mention the Terrorism Act as a reminder that preventing criminal proceeds going to fund terrorist activity grows ever more significant.

Our primary obligations

Our obligations are essentially three-fold:

- to take appropriate measures to avoid our businesses being used for money laundering (and terrorist financing);
- to report it where we suspect it is occurring (SARs); and
- to keep adequate records so that suspicious activity can be properly investigated and prosecuted.

KYC: Know your customer/client also known as CDD: client/customer due diligence

Knowing our client/customer and performing client due diligence is at the heart of measures we must adopt in order to be compliant and our obligations are set out fairly comprehensively in Regulations 5-15 of the 2007 Money Laundering Regulations.

What is required?

Regulation 5 explains what is required for ordinary customer due diligence, namely: identifying the customer/client and verifying that identity through a

reliable and independent source; and where there is a beneficial owner who is not the customer/client, identifying that owner and taking adequate measures to verify that identity on a risk-sensitive basis.

We are also required to obtain information on the purposes and intended nature of the business relationship.

When is it required?

Regulation 7 provides three triggers for requiring CDD measures to be undertaken:

- when (actually before) we establish the business relationship or carry out a transaction;
- when we suspect money-laundering or terrorist financing; and/or
- where we doubt the veracity or adequacy of the documents, data or information previously obtained for the purposes of identification and verification.

Regulation 8 deals with ongoing monitoring (see later/below) but Regulation 7 also requires us to apply customer due diligence measures at other appropriate times to existing customers.

How do we conduct CDD?

The regulations say what we should do and when but other than to emphasise that we must do so on a risk sensitive basis they do not prescribe how we should do this.

Each industry sector and the regulatory bodies in those sectors publish guidance notes on best practice, whilst seeking not to detract from the all-important theme that we must adopt a risk sensitive approach. What is appropriate for one risk factor may not be for another. I still advocate a face-to-face meeting with the client and production of ID documents where possible and proportionate, but it is difficult in the modern world to think of a better system than that such as is offered by CallCredit where, for a few pounds, you can search the enormous databases available to obtain reliable and independent verification of a client's identity and, where necessary, beneficial owners. Such searches can also help you in assessing risk depending on the search criteria adopted.

To Emphasise: CDD means not just knowing our client or customer but also their business relationship with us, assessing the risk of exposure to money laundering from that client or relationship and adopting appropriate measures to meet that risk. We are then obliged to monitor it during the relationship.

Ongoing monitoring

We have already seen that Regulation 7 requires customer due diligence measures to be applied at other appropriate times to existing customers. Regulation 8 enforces this obligation and describes ongoing monitoring as meaning the scrutiny of transactions undertaken throughout the course of the relationship so as to ensure that the transaction is consistent with the relevant person's knowledge of the customer, his business and risk profile and keeping the documents, data and information obtained for the purpose of client/customer due diligence measures up-to-date.

Given that Regulation 20 obliges us to establish and maintain appropriate and risk-sensitive policies and procedures in relation to our obligations, it is essential that you undertake regular documented reviews of your client/customer business relationship if you are not already doing so.

Suspicious activity reports (SAR)

We should all now be familiar with these. Our obligations arise out of part 7 of POCA and in particular sections 330, 331 and 332. SAR's are now made to the National Crime Agency (**NCA**) and according to its first published annual report on SAR's there were over 381,000 in year 2014/15, over 83% of which came from banks. Other financial institutions accounted for a further 12% leaving all other sectors responsible for just 5%.

The regime provides that businesses in the regulated sector must appoint a nominated officer, and staff working in that business are provided with a defence from prosecution if they report their suspicions to the nominated officer, who in turn must then decide whether to disclose those suspicions to the NCA by way of a SAR.

Nominated officer's (aka Money Laundering Reporting Officers - MLRO's-and I am one) must make a disclosure to the NCA where they know or suspect money-laundering, or terrorist financing (a subjective test) or where there are reasonable grounds for suspecting suspicious activity (an objective test).

It is worth remembering also that anyone can make a disclosure pursuant to section 338 of POCA where they suspect money-laundering and section 338 of POCA provides them with a defence if they go on to otherwise commit one of the substantive money laundering offences described in sections 327 to 329 of POCA.

Note also that there are defences for delaying or not making a disclosure but I advise non-lawyers to seek legal advice before making such a decision given the penalties for failing to do so. Those of you who are lawyers will know that one of the reasonable excuses for not making a SAR is that the information came to you in a situation covered by Legal Professional Privilege, a defence not open to other professionals.

The NCA report I have referred to is worth reading, and can be viewed on the NCA website.

Studying the report, it is pleasing to note that the confidentiality of SARs promised by the regime is working well and that only two breaches of the confidentiality of reports are recorded.

From my own experience, the consent to proceed is working reasonably well and the seven-day target promised is being met by the NCA, who say that their average response is 3½ days.

Finally, once a disclosure has been made, don't forget the anti-tipping off requirements of section 333 POCA which always cause difficulties for professional advisors putting us in conflict with our duties to keep our clients informed.

Record keeping

Regulation 8 requires us to keep our AML records up to date and Regulation 19 provides that we must keep those records for the specified period, which is 5 years from the end of the business relationship or when the occasional transaction is completed. The records specified are the CDD documents and records supporting the nature of the business relationship. Keeping business records is second nature to most if not all of us in the regulated sector and given the e-storage facilities available to us it is will be no easy task to defend an allegation of failing to keep adequate records.

Keeping compliant

There has been relatively little substantive change to the legal framework outlined above for some years now and the legislation has grown into its existing state since the establishment of the Financial Action Task Force (**FATF**), in 1989 and the First EU Directive in 1991. There is out there a wide ranging network of advice and guidance issued by government and law enforcement agencies and our professional and regulatory bodies. It is essential that you obtain the AML guidance notes specific to your sector and that you subscribe to relevant bulletins in relation to anti-money laundering and terrorist financing. I also recommend attending relevant courses and seminars and (of course!) consulting relevant experienced professionals such as myself should you need more detailed or tailored help in keeping compliant.

There simply is no excuse for not keeping up-to-date given the enormous amount of material and training available.

And don't forget the need to train all staff in ML and TF awareness (regulation 21).

The Fourth EU Directive

Was enacted in June 2015 and requires full implementation by June 2017. The current thinking is that it should not be too difficult to assimilate the changes into our current framework as the emphasis is very much on expanding the concept of ultimate beneficial ownership and the need for enhanced customer due diligence in that area. One significant change is the need to establish central registers of corporate ownership details

It also expands the definition of Politically Exposed Persons to those operating within the boundaries of the United Kingdom and for those involved in the gambling sector; it takes the regulations beyond just casinos.

Summary

I will finish where I started. Those of us who work in the regulated sector and those of us who are compliance or reporting officers in that sector are no longer regarded as businessmen; we are gatekeepers. We are required and expected to take risk based measures to avoid our businesses being targeted by criminals to launder the proceeds of criminal conduct or to fund terrorism. If despite such measures we are unlucky enough to fall foul of the activities of terrorist funders or money launderers, we need to be able to show that we have adopted all the measures required of us, that if there were reasonable grounds for suspecting ML, we reported it and that we have kept full, proper and adequate records of the measures taken by us and our appropriately trained staff.

If we can't do all of this then we may well face civil, regulatory and even criminal sanctions as well as loss of business reputation and goodwill.

Note and disclaimer. This is the text of a short oral presentation and must not be taken to be a definitive guide on any part of the law in relation to money laundering and terrorist financing. There are many exceptions to the general principle's outlined above. Please seek professional help on a retained basis should you have the need to do so.