AFEP newsletter

March 2017

CHAIRMAN'S COMMENTS

Dear Members,

All firms will be more than well aware of the forthcoming legislation and we have provided a key dates timetable below. As usual the Executive has been incredibly busy keeping abreast of the various consultations. The industry has been very well represented by Millie Richardson, Richard Creed, Jude Bahnan and AJ Penniston on the commercial forwards test, all of the scenarios being suggested having been provided by this team. We await the final outcome, which needs European approval before it can be finally issued. In the meantime, the thorny issue of the treatment of NDFs is still being debated. Jude has provided an update on the gateway for those firms who may need to obtain investment firm permissions as a result of the MiFID 2 changes. To reiterate, the FCA has requested to have your applications in as soon as possible and in any event, before end of July 2017.

The fraud focus has gathered speed with the introduction of CiSP and the support we have received from the Met Police and Project Falcon. Kam Biring has been instrumental in building these relationships and getting our CiSP membership off the ground. There are a number of firms now in the community and we encourage all firms to join.

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 latest consultation closes 12 April 2017 ready for the final Regulations to be issued in June. A high level summary is contained below. As the Regulations bring new requirements for tax crimes we are putting some focus on this area. Kam has written a brief article on VAT fraud in this month's and we are looking into expert input on tax crimes with a view to having a speaker in June or September.

GDPR has gained momentum and Steph Innes from MMS brings us up to speed on the latest developments. Whilst Richard Creed has summarised the key points of the Criminal Finance Bill which has reached Lords committee stage where line by line examination of the Bill commences 28th of this month.

Firms will receive calls and requests for information from various Law Enforcement agencies. Releasing data can sometimes be delayed subject to a formal request being made and identities of Accredited Financial Investigators being verified. To counter this, the National Crime Agency have rolled out the Financial Investigation Support System (FISS) which stores the Financial Intelligence Gateway List. Kam has provided guidance on FISS below.

Looking forward we will continue to take an active part in helping to shape the legislation as it is transposed into law as well as inform the guidance which necessarily accompanies it. All member firms are encouraged to take an active part in consultations as we know, in this regard, size of response really does matter!

Francesca Maritan

Chairman

VAT Fraud and Online Sellers – risks and controls to consider

Kam Biring

Tax evasion and tax avoidance is often a misunderstood concept within the Payment Services and E-Money Industry. Tax evasion is the "illegal non-payment or underpayment of tax" while tax avoidance is "the arrangement of one's financial affairs to minimise tax liability within the law.

While tax evasion has always been a crime in the UK, its inclusion as a predicate offence into AMLD 4 will be an obvious concern for most firms who will now need to have controls in place to detect any money laundering linked back to possible tax evasion. While there are various techniques to commit VAT fraud, some of the common ones that firms need to be aware of are below:

- Cash based business with no VAT registration
- Business payments going through personal accounts to reduce the taxable turnover of a business therefore resulting in payment of less tax
- Missing Trader Fraud - is the theft of VAT from a government by organised crime gangs who exploit the way VAT is treated within multi-jurisdictional trading where the movement of goods between jurisdictions is VAT-free
- Non-payment of VAT by overseas sellers in foreign jurisdictions who supply goods to the UK.

VAT fraud and Overseas sellers are an increasing risk to firms and something that the Government and HMRC are taking action on. An article published by the Guardian in November 2016 posted that the Government is launching an investigation into large-scale companies that provide platforms for these overseas sellers to sell their products while circumventing the tax rules.[1] Payment firms that support overseas sellers may very well be caught up in this net so understanding the risk and the simple controls that you can put into place to evidence your firms are not complicit in tax evasion are detailed below.

How it works:

Non-Established Taxable Persons (NETPs) is the official term for businesses from outside the UK who are warehousing and dispatching goods from the UK to customers in the UK. HMRC rules from 2012 state that all NETPs supplying goods located in the UK are required to register for VAT when they make their first supply of goods or services, regardless of the value – this is separate to the VAT registration requirement for UK firms where a minimum taxable turnover amount is required.[1]

NETP's who are not VAT registered are evading tax on any sales that are made and therefore, post 4MLD, monies linked to their sales could constitute money laundering which would impose a legal obligation on all firms to ensure the appropriate disclosures are made to the Financial Intelligence Units.

Controls:

The basic controls that a firm can put in place to ensure that they are controlling this risk are similar to existing controls that a firm will have in place a clear understanding of their business clients activities as part of their CDD framework. Key questions that a firm should be asking of their clients, should consist of the below:

- Are they VAT registered?
- Can that VAT number be validated?
    - Firms can use the VIES VAT number validation tool to validate VAT numbers that have been issued http://ec.europa.eu/taxation_customs/vies/vatResponse.html
- Is the client's turnover with your firm over the taxable turnover threshold (currently 83,000.00 in any 12 month period)?
    - If so do you hold a valid VAT number for the firm?
- Is the client's company incorporated outside of the EU but selling into the UK?
    - If so are they possibly a NETP?
- Where is the company's warehouse and dispatching completed from? Is it from the UK?
    - If so are they possibly a NETP?

The above controls can be embedded into a firm's CDD policy and process and will ensure that firms have procedures in identifying potential tax evasion, which may constitute money laundering.

References

[1] https://www.theguardian.com/business/2016/dec/21/mps-vat-fraud-amazon-ebay-public-accounts-committee
[2] http://www.vatfraud.org/invasion-of-the-netps/

4MLD summary

Francesca Maritan

The Fourth Anti-money Laundering Directive comes into force June 2017. HMRC have confirmed new guidance is to be issued in line with the new legislation. JMLSG Guidance will be also be available from the BBA after the Directive has been transposed. In advance, here is a quick summary:

Home and Host Responsibilities

Under the 4MLD, all branches and subsidiaries operating in other Member States will need to ensure that those establishments respect the UK national provisions. Firms will also be required to review their arrangements where reliance is placed on the head office to ensure compliance with host requirements.

New Obliged Entities

Virtual currency exchanges and wallets will become obliged entities.

Customer Due Diligence

Simplified Due Diligence will no longer be applicable in most circumstances. 4MLD will update the current list of circumstances where simplified customer due diligence would apply. Before applying simplified measures, firms will be required to consult the lower risk situations set out in Annex II of the Directive.

Similarly firms will need to consult the factors listed in Annex III of the Directive to determine where transactions may require enhanced due diligence. Higher risk situations will include: transactions involving asset holding vehicles and cash-intensive businesses, those where unusual or apparently unnecessarily complex ownership structures are in place and those associated with higher risk jurisdictions.

Beneficial Ownership

Member States shall ensure that corporate and other legal entities incorporated within their territory are required to obtain and hold adequate, accurate and current information on their beneficial ownership, including the details of the beneficial interests held. Such information should be held on a central register accessible to competent authorities. The scope of the Directive is broad in that the requirements apply to trusts and other legal entities rather than just companies. The UK has already changed its national law to require all companies to report beneficial ownership information to a central register.

PEPs

The definition of PEPs has been widened to include domestic individuals occupying prominent public positions, in addition to those from abroad and EDD will always apply. Firms will now also be required to apply EDD on PEPs for at least 18 months after the individual ceases to be a PEP.

Suspicious Activity Reports

Firms will now be required to report any suspicious transactions, including attempted transactions.

Tax crimes

4MLD includes tax crimes as a predicate offence for money laundering.

One-Off Transactions

Traders in high value goods must undertake customer due diligence when dealing with cash transactions of EUR 10,000 or more (decrease from EUR15, 000).

Gambling

The requirement for certain entities to carry out CDD has increased e.g. from just casinos across the entire gambling sector. There is an obligation for providers of gambling services posing higher risks to apply customer due diligence measures for single transactions amounting to EUR 2,000 or more.

National Risk Assessments

Member states are required to carry out a national risk assessment of its exposure to money laundering and terrorist financing. Risk assessments must be documented, kept up to date and made available to the competent authorities and to each other member state. HM Treasury published the first UK national risk assessment in October 2015. And it can be found here: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf

Written Risk Assessment

The 4MLD introduced new requirements on firms to take appropriate steps to identify and assess the risks of money laundering and terrorist financing and to document its methodology. These written risk assessments must be kept up to date and be available to the Regulator upon request.

Third Country Equivalence Regime

A list of 'equivalent jurisdictions' will be scrapped and instead, the European Commission will identify high risk non-EU countries with strategic deficiencies in AML/CTF standards, requiring firms to apply EDD when dealing with persons or entities established in these countries and further requiring such firms to review their country risk assessments.

Record Keeping

Member States will still be required to ensure that firms retain client information for the maximum period of five years after the end of the business relationship with the client. However, there is now a provision for a potential extension of the retention period for up to an additional five years in certain circumstances.

Key dates for members to be aware of

April 2017	Publication of draft revised Approach document for PSD II
26 June 2017	MLD 4 and FTR 2 in force
28th June 2017	Publication of final Policy Statement of MiFID II Guidance on FX Forwards and the "means of payment' exemption
3 July 2017	Deadline for submission of **complete** applications for Authorisation or Variation of Permission before MiFIDII in force
3 Jan 2018	MiFID II / MiFIR in force
13th Jan 2018	PSD II in force
25th May 2018	GDPR comes into force
13th July 2018	Deadline for existing payment institutions to comply with new PSD II Title II requirements

The General Data Protection Regulation – An Update

Steph Innes, Associate, Mclay Murray & Spens LLP

Further to the General Data Protection Regulation ("**GDPR"**) discussion at the AFEP Member Meeting in December 2016, some further updates have become available with the publication of European level guidance.

Impact of the GDPR

As outlined in December's discussion, the GDPR will take effect on 25 May 2018, applying automatically in all Member States of the EU. The UK will still be part of the EU when the Regulation comes into force, therefore Brexit will not delay or prevent UK GDPR implementation. Although there may be minor changes to how the rules apply to the UK when Brexit actually takes effect, it is anticipated that these will be minor.

To summarise, the reach of the GDPR will be much greater than the Data Protection Act 1998 (**"DPA"**) as: (i) it will apply directly to data processors as well as data controllers; and (ii) it will apply to non-EU based entities that offer goods or services to EU data subjects and/or monitor behaviour of EU data subjects (for example, by using cookies). Fines for non-compliance will increase significantly, and there will be more stringent requirements in terms of governance of personal data. The requirements for collecting data subject consents will also become stricter - the ICO have now published their draft consent guidance for public consultation, with finalised guidance expected to follow. Some organisations will be required to hire a Data Protection Officer. There will also be some changes to cross-border transfer rules, and to data subject access request rules. The GDPR will give data subjects a new right to be forgotten, a right to data portability and reporting of data breaches will become mandatory.

Discussion during and after December's presentation highlighted specific concerns over potential changes to the rules regarding the use of personal data for profiling, or credit searches. The GDPR provides that data processing may constitute 'profiling' where: (i) there is an automated processing of personal data; and (ii) that personal data is used to evaluate certain personal aspects relating to the data subject (in particular, among other things, to analyse the data subject's economic situation). The key points to note are:

Data subjects have the right to object to profiling, and to avoid profiling-based decisions. Specifically, data subjects have a right to avoid being subject to a decision based solely on profiling that produces legal effects; for example, the automatic refusal of an online credit application without any human intervention.

However automated decisions can still be made provided the data subject gives their explicit consent to the use of their data in profiling; and

All permissible profiling must be fair and transparent, use appropriate statistical procedures, secure all personal data, and minimise the risk of error.

The "explicit consent" requirement sets a higher bar than under the old rules - it is even more important to ensure consents are obtained correctly. The European Data Protection Board is expected to issue guidelines, recommendations and best practices specifying the criteria and conditions for decisions based on profiling in due course, which will also play an important role in ensuring data used for credit searching is handled in a compliant manner.

Other Developments since December

Since December's discussion, EU level guidance has now been published on: (i) data portability; (ii) data protection officers; and (iii) identifying a controller or processor's lead supervisory authority. The key messages are as follows:

Data portability - organisations will be required to offer a direct download opportunity for the data subject, and an option for the data subject to transmit the data to another controller.

Data Protection Officers - the DPO should not be a person in a senior position, and the DPO should retain some independence from senior management. Specifically, Chief Executives, CFOs, Heads of HR, Heads of Marketing and Heads of IT should not be the DPO.

Identifying the lead supervisory authority - where an organisation has multiple establishments, the lead authority will be determined by where the decisions regarding the purposes and manner of the processing takes place. This will be relevant for groups of companies with activities in different Member States.

Further guidance on other GDPR topics is expected from the A29WP and the ICO throughout 2017.

Privacy and Electronic Communications Regulation

The EU Commission also published the proposed new E-privacy Regulation on 10 January 2017, which broadly does the following:

Marketing consents rules remain largely the same. Organisations will need an opt-in consent, other than for data collected in course of a sale (where an opt-out can be used instead). There are new transparency requirements with regard to direct marketing calls;

There are new specific rules about the use of communications data and communications metadata;

In terms of cookies, there will be an exception to the need for data subject consent in respect of first party analytics cookies (though notably not third party analytics). This means that websites and apps using third party analytics, such as platforms like Google Analytics, will still need consent; and

Potential fines under the E-privacy Regulation will be of the same level as the GDPR. The Regulation also comes into force on the same date (25 May 2018).

Recommendations

We are currently advising clients preparing for GDPR compliance, commonly by way of fixed cost Data Protection Audits. The Audit includes diligence on your practices and procedures, and a report on key findings and recommendations. Please contact us if you are interested in this service and we will be happy to assist.

CISP Registration

AFEP has connected with the Metropolitan Police and CER UK to register on CISP (Cyber-Intelligence Sharing Partnership). CISP is a secure forum owned and managed by CERT UK who are the lead authority in the UK in detecting and preventing cybercrime attacks on businesses. AFEP will be sharing all future cybercrime intelligence via CISP in order to engage with the industry and law enforcement via a safe and secure forum. The steps to registration are below.

Registration with CISP:

To register with CISP a pre-condition is that you must be an FCA regulated firm or working in law enforcement.

Registration is completed online by following the below link and registering the regulated firm first (individual user applications are completed after the firm is registered on CISP).

https://www.ncsc.gov.uk/cisp/register/organisation

A pre-condition to registration is that you will require a sponsor – a sponsor can be any of the following:

- Existing member
- Law enforcement individual
- Trade body member

AFEP has confirmed with the Metropolitan Police that the below sponsor details can be used for all AFEP members – DC Chris Young is the administrator of the CISP Registration Process and has confirmed that he is happy for his details to be used which are listed below

DC Christopher Young . **Cyber Protect Officer** Christopher.Young@met.pnn.police.uk

Telephone 020 7230 8610. Address Rm 01.05, Ocean Block, Cobalt Square, 1 South Lambeth Road, London, SW8 1SU.

If you have any problems in respect of registration, please contact El Martin.

Upcoming Member Meeting

Wednesday 14th June

Venue: TBC closer to the time

Time: 5.00pm

Agenda: The focus of the member meeting will be jurisdiction and post Brexit with an update from the Executive Committee. The meeting will be followed by the AFEP annual social event.

FISS Registration

Kam Biring

As regulated firms, on occasion we will receive calls and requests for information from various Law Enforcement agencies. Releasing data can sometimes be delayed subject to a formal request being made and identities of Accredited Financial Investigators being verified. To counter this, the National Crime Agency have rolled out the Financial Investigation Support System (FISS) which stores the Financial Intelligence Gateway List.

Details of FISS are below

Confirming identities using the FIG list

Access to search the FIG list is via the Financial Investigation Support System (FISS) website, which is run by the NCA's Proceeds of Crime Centre (PoCC). We will create FISS accounts for the individuals specified on the form.

We are required to forward completed forms to the Financial Conduct Authority (FCA) for verification. We will then contact the nominees who will each be requested to confirm acceptance of our terms of usage, prior to receiving individual login details.

We will also record the details of the Main Contacts and Heads of Units for follow-up correspondence and to complete regular checks on the continuing validation of all your staff with FIG access.

Your department contacts

To assist Financial Investigators and Financial Intelligence Officers with making enquiries (e.g. pre-order / financial intelligence), we produce a contacts list for all registered Regulated Sector organisations.

The contact details of the nominees on the application form will be included on the list, unless indicated otherwise. Please ensure however that at least one clear contact point is made available.

Registration Process

Please note that regulated sector organisations that wish to access FISS have to complete and return a completed application form. A copy of which can be requested by emailing the following email address - fisshelp@nca.x.gsi.gov.uk

We inform applicants that:

FISS Support Desk- Further links on FISS are below for your reference

Proceeds of Crime Centre

Economic Crime Command

National Crime Agency
Units 1-6, Citadel Place, Tinworth Street, London SE11

Email: fisshelp@nca.x.gsi.gov.uk

Web: https://fiss.nationalcrimeagency.gov.uk

www.nationalcrimeagency.gov.uk

www.facebook.com/NCA

Criminal Finance Bill

Richard Creed

Richard Creed provides a brief synopsis of parts of the bill below:

Amending the suspicious activity reporting (SARs) regime (clauses 9 and 11 of the Bill):

- Clause 9 of the Bill amends POCA to extend the current 31 day moratorium period for the National Crime Agency (NCA) to investigate SARs. Clause 9 would allow an extension of the moratorium period, by court order, up to a maximum period of no more than 186 days from the end of the initial 31 day moratorium period.
- Clause 11 of the Bill also gives the NCA the power to request further information from any person in the regulated sector following receipt of a SAR, or where it has received a request from a financial intelligence unit (FIU) in another country.

Enhanced information sharing between entities in the regulated sector (clause 10 of the Bill).

- Clause 10 of the Bill amends POCA to provide a legal gateway for the sharing of information between entities in the regulated sector with a view to encouraging better use of public and private sector resources to combat money laundering. Although existing data protection legislation allows information to be shared for preventing and detecting crime, regulated entities are concerned that there should be express legal cover that is directly related to the anti-money laundering (AML) regime to reduce the risk of civil litigation for breach of confidentiality.
- Clause 10 allows regulated bodies to share information with each other where they have notified the NCA that they suspect activity is related to money laundering. This will enable the submission of "super SARs" (joint disclosure reports), which bring together information from multiple reporters into a single SAR that provides the whole picture to law enforcement agencies. Initially, this measure will extend to financial sector organisations. It will be extended to all entities in the regulated sector in due course.

New civil recovery powers for the FCA (clause 16 of the Bill).

- Clause 16 of the Bill amends POCA by inserting provisions giving the FCA the power to recover property in cases where there has not been a conviction, but where it can be shown in the balance of probabilities that the property has been obtained through unlawful conduct. This would enable the FCA to take proceedings in the High Court to recover criminal property without the need for the owner of the property to be convicted of a criminal offence.

Extending certain powers to apply to investigations relating to terrorist property and financing (Part 2 of the Bill: clauses 29 to 35).

- The powers in the Bill relating to enhancing the SARs regime and information sharing, among others, would be extended by Part 2 of the Bill (clauses 29 to 35) to investigations relating to terrorist property and financing.

New corporate offences of failure to prevent the facilitation of tax evasion (Part 3 of the Bill: clauses 36 to 44).

- Currently where, for example, a banker criminally facilitates a customer to commit a tax evasion offence, the banker commits a criminal offence, but the bank does not. This is so even in cases where the bank tacitly encourages its staff to maximise profits by assisting customers to evade tax. However, Part 3 of the Bill (clauses 36 to 44) introduces two new offences that will aim to hold legal persons, like the bank in this example, to account for the actions of their staff. Rather than focusing on attributing the criminal act to the company, the offences focus on, and criminalise, the company's failure to prevent those who act for or on its behalf (associated persons) from criminally facilitating tax evasion when acting in that capacity.
- It would be a defence for the company if it could show that it had in place reasonable prevention procedures, or that it was not reasonable to expect such procedures. Under clause 39 of the Bill, the Chancellor of the Exchequer is to produce guidance to help relevant bodies to develop reasonable prevention procedures. The Chancellor also has the power to endorse guidance produced by others, for example, trade associations.

FX FORWARDS: MiFID II Gateway opens

Jude Bahnan

FCA has opened the MiFID II gateway for those firms who think they might be affected by the changes in the treatment of FX forwards under MiFID II. We would urge any firm that thinks it might be affected by these changes to review the proposed guidance from FCA on FX forwards to see if they need to apply for investment firm permissions. If so, FCA have urged any firms affected to apply as soon as possible, and in any event before the end of July if they wish to be authorised in time for 3 Jan 2018 when MiFID comes into force.