Association of Foreign Exchange
and Payment Companies

October 2017

CHAIRPERSON'S COMMENTS

As we approach the end of the year, we seem to be busier than ever making preparations for 2018. The Executive Team remain very busy keeping up to date with all the regulatory and legislative changes; attending briefings and meetings on behalf of the AFEP. In particular MiFID II, PSD2, GDPR and the Criminal Finance Act are high on the agenda with changes imminent.

The October 2017 newsletter will focus on these key changes and help you prepare for the December member meeting where we are in the process of securing the FCA to speak on MiFID II and PSD2.

The amount of changes facing our industry doesn't seem to be fading and we encourage all members to take heed of the advice and guidance in this Newsletter and their own legal advice to ensure compliance and best practice.

On behalf of the Exec, it's been a pleasure representing the AFEP during the past 12 months, and we look forward to another busy 12 months!

Francesca Maritan

Chaiperson AFEP

CRIMINAL FINANCE ACT 2017

Jason Collins, Partner at Pinsent Mason, talked us through the Criminal Finance Act at the September Member meeting. With the legislation coming into force in October 2017, we have summarised the key points of his presentation as an important reminder.

The Act makes companies liable for failing to prevent their employees from facilitating tax evasion. The penalties are harsh; a criminal record, unlimited fines and confiscation, it is definitely one to take seriously.

Prosecution under the legislation requires 'fraudulent' tax evasion with a criminal intent: dishonest attempt not to pay tax which person knows to be due (or reckless). Be warned that 'turning a blind eye' can amount to the necessary dishonest intent.

HMRC Guidance issued six guiding principles for prevention:

- Risk assessment
- Proportionality of risk-based prevention procedures
- Top level commitment
- Due diligence
- Communication (including training)
- Monitoring and review

It is important you have your risk assessments up to date, have trained your staff to be aware of the risks – particularly looking at:

- Private individual/company
- High tax country of residence
- Structure potentially used to hide activity, e.g. cross-border, especially in a low tax jurisdiction

Managers should also be aware of close relationships between employees and customers which may put the Company at risk, but remember this is not a test of suspicion, but one of intent.

For more in depth information, Jason can be contacted at Pinsent Masons on 0207 054 2727 or via email Jason.Collins@pinsentmasons.com

Registered address c/o 1 Fleet Pl, London EC4M 7RA. Company No. 07917853

STRONG CUSTOMER AUTHENTICATION (SCA)

Despite the ongoing consultation regarding SCA, the RTS from February 2017 and the European Commission response has not yet entered into the EU ledger so the 18 months has still not started. It is however worth being prepared in advance as the requirements look likely to have weighty reporting procedures.

The European Commission response in July confirmed 4 substantive changes which are worthy of note:

1. Independent auditing of the security measures in cases when transaction risk analysis exemption is applied

To ensure objectivity in the application of this exemption between different providers, as well as quality of reporting and independent verification, statutory auditors should perform an audit of the methodology, risk model and reported fraud rates.

2. New exemption to strong customer authentication for certain corporate payment processes – the main change

New exemption for SCA where certain corporate payments use dedicated payment processes that achieve a level of security. This will allow authorities to establish they meet PSD2 criteria.

3. Fraud reporting by payment service providers directly to EBA

The EBA will have aggregated data as well as individual fraud data and reports from payment service providers

4. Contingency measures in case of unavailability or inadequate performance of the dedicated communication interface

Ensures that unavailability/poor performance of the dedicated interface doesn't prevent payment initiation services & account information service providers from offering their services.

Banks should offer secure communication through user facing interfaces as contingency. PSD2 still applies and usage need to be documented and justifiable and reported to authorities.

These notes have been informally drafted and circulated to AFEP members confidentially to allow them access to the content of the Stakeholder Liaison Group Meeting which was held in October 2017.

If you have any questions regarding PSD2, the AFEP recommend you contact the FCA or take independent legal advice.

- **The FCA emphasised that firms should consider responding to the EBA fraud consultation** (closes on 3rd November) as the requirement are potentially onerous.

- **The FCA is open for applications under PSD2 (the PSRs 2017)**

From 13 October 2017 businesses can apply to be authorised or registered under the Payment Services Regulations (PSRs) 2017, or the Electronic Money Regulations (EMRs) as amended by the PSRs 2017.

Firms already authorised or registered under the PSRs 2017 or the EMRs can also submit applications for re-authorisation or re-registration. Authorised payment institutions, authorised e-money institutions and small e-money institutions must submit an application by 13 April in order to continue providing payment services or issuing e-money beyond 13 July 2018. Small payment institutions must do this by 13 October 2018 in order to continue providing payment services beyond 13 January 2019.

All affected firms must submit a complete application via the FCA Connect system. It can take up to 3 months to determine an application but could take up to 12 months if an application is not complete.

Find out more on how to prepare for PSD2 if you want to become, or you are already a payment institution or an electronic money institution.

- **Get ready for 13 January 2018**

PSD2 introduces a number of new requirements around how firms must treat their customers, handle complaints, and the data that is reported to us. The majority of the new regime will apply from 13 January 2018. You can read in full about our approach to regulating firms under PSD2 in the PSD2 Approach Document and Policy Statement.

To help businesses identify the key changes that are relevant to them resulting from PSD2 we have launched the PSD2 Navigator. The online decision tool directs firms to relevant information and details of what they need to do to be PSD2 compliant.

Inaddition to capital / ability to meet liabilities as they fall due, the FCA indicated that they will focus on how those businesses seeking reauthorisation will meet new requirements including:

1. Procedures for incident reporting
2. Processes for sensitive payment data
3. Arrangements for business continuity
4. Security policy (risk assessment / mitigation)

- **Firms wishing to vary permissions to add AISP / PISP can apply for a variation at the same time** as applying for reauthorisation. Please note that firms are not able to apply for variation prior to resubmission as the new permissions are only available under PSD2 authorisation

- Firms are encouraged to **read the Approach document as well as the Policy Statement** (this was raised particularly in reference to outstanding questions on safeguarding);

- **PISP / AISP permissions require indemnity insurance or equivalent guarantee** – FCA believe some insurers have now developed suitable cover – will send further details as they obtain them;

- **They have updated the guidance on limited network exclusion** and there will be further updates to the SLG in the future

- **The SLG discussed complaint handling**, particularly the difference in definition of business days in DISP and PSD2. The FCA clarified that there are 2 definitions of complaint handling in DISP and the PSD 2 definition only applies for the 15 day rule. The FCA confirmed for rest of DISP the other definition applies and the group raised that this is operationally difficult and equally hard to explain to consumers.

- **FCA are aligning with supervision of other sectors**. There is a review of the supervision approach being undertaken across the FCA and the key change is moving to and "emphasis on harm" approach. Approach will be more proactive and less complaints led with more thematic reviews

- The FCA said they would **welcome information on firms operating without a relevant license** to enable them to investigate and you can raised this with the FCA directly or via the AFEP.

- **FCA wants to remain ahead in respect to changes in the industry. They expect to make further changes going forward** (particularly as the RTS remain outstanding) so would like to use the group to continue to raise any issues with the approach document identified by industry.

The AML Regulations came into law on 26 June 2017 to replace the Money Laundering Regulations of 2007 and Transfer of Funds (Information on the Payer) Regulations 2007. The intention is for MLR 2017 to improve upon and plug certain gaps in MLR 2007, including:

- prescribing the approach to customer due diligence and removing the automatic application of 'SDD'
- seeking to prevent new means of terrorist financing, including through e-money and prepaid cards
- improving transparency of beneficial ownership of companies and trusts and persons of significant control therein
- effectively enforcing sanctions and specifying high risk jurisdictions
- apply to a relevant person and its subsidiaries irrespective of where they are located.

The relevant persons from Board level down need to adopt more detailed risk-based approach towards anti-money laundering – particularly around due diligence. The regulations place particular emphasis on:

- **Board familiarisation** and appointment of board member with specific responsibility for AML Compliance
- Appointment of an **AML Compliance Officer** as well as the Nominated Officer (although can be the same person)
- Review and revision of AML **written risk assessments & policies/procedures**
- Planning **training** for front line staff conducting AML

ANTI MONEY LAUNDERING KEY CHANGES

- **General risk assessment** – more prescriptive in requirements and imposes obligations for HMT & Home Office to conduct national risk assessments as well as relevant persons
- **Risk mitigation policies** - must be proportionate and include internal controls and Board Member responsible for AML
- **Due diligence** – MLR 2017 restricts use of simplified customer due diligence & includes 'black list' of high risk juristictions making enhanced DD compulsory
- **Beneficial Ownership:** Compels UK corporate bodies & trusts to provide information on demand
- **Third parties & Reliance**– MLR clarifies circumstances for 3rd party reliance and compels the 3rd party to provide the data it has obtained immediately on request
- **Politically Exposed Persons** - MLR 2007 requirements around foreign PEPs now apply to local PEPs – enhanced DD necessary
- **New Criminal Offence** – recklessly making a false/misleading statement, in the context of a money laundering investigation, punishable by fine and/or up to 2 years in prison

Registered address c/o 1 Fleet Pl, London EC4M 7RA. Company No. 07917853