Overview

- The EMA
- The scope of mobile payments and of money laundering
- Regulatory obligations for the regulated sector
- The challenges for mobile and other new payment products
- An approach to resolution
- Case study: electronic money in the EU
- Counter terrorist financing
- A note on the transfer of airtime

Members of the EMA

Scope of mobile payments

- Mobile payments encompass a wide range of payment services
- Consider three scenarios that are typical of current challenges:
  - Mobile payments used primarily to purchase digital goods and services but increasingly widening in the range of use
  - Mobile payments used to affect money remittance either intra-country or cross border
  - Mobile airtime account funding by third party related individuals, as a means of remitting value and as a medium of exchange

Scope of money laundering

- Conventional conceptions relate to the transformation of the proceeds of crime into apparently legitimate income, usually described as placement, layering and integration
- The prescribed offences relate to all parts of the activity such as concealing arranging, acquiring and possessing proceeds of crime
  - Many legislative frameworks limit the scope of offences to proceeds arising from 'serious crime' rather than 'all crime'
  - Increasingly, countries are adopting an all crimes approach; meaning that the proceeds of any crime can give rise to an offence of ML

ML and the regulated sector

- The obligations on the regulated sector extend beyond the predicate crime of money laundering, and require the to deterrence and detection of ML
- For an 'all crimes' definition of money laundering, detection will relate to proceeds of any crime, from the use of stolen credit cards to drug dealing
- The obligation to detect and report instances of suspicion of money laundering relates therefore not only to the conventional conception of money laundering but to transfers of funds involving any kind of fraud or other crime
ML, regulated sector obligations

• The obligations on the regulated sector are encapsulated in the FATF recommendations and special recommendations which are then promulgated in national legislation

• They relate to a range of provisions including:
  - Undertaking customer due diligence (DD), both initial and ongoing
  - Having systems to monitor and detect suspicious activity
  - Reporting such activity to the relevant Financial Intelligence Unit (FIU)
  - Keeping records of transactions and of evidence of DD for a given period of time
  - Training and informing relevant personnel of the legislative obligations and how ML may take place

Obligations and mobile payments

• Whilst all the obligations apply to a mobile payment service providers, two give rise to particular challenges
  - The first is undertaking due diligence of consumers (rather than business customers)
  - The second is reporting on suspicious activities where the obligation is an ‘all crimes’ approach to ML.

Why DD often poses a challenge

• Mobile payments typically comprise small values; ranging from a few cents to $100 or more; with values under $10 predominating
  - The relative cost of undertaking conventional due diligence on customers at the outset is significant; perhaps as high at 10-20% of the value of the transaction

• Where there is no prior relationship with a customer, a DD step at the outset can act as a barrier to take-up of the new service

• The means of undertaking due diligence varies from one country to another, whether face to face or remotely.
  - In developed countries the availability of data on customers varies considerably
  - In developing countries, even paper documents are not always widely available

Solution: a two pronged approach

• In order to resolve the DD challenge practically, two factors must be addressed:
  - The legal obligations to undertake DD must be met
  - The risk of ML taking place in practice must be mitigated

The legal obligation

• The requirement relates to initial DD on customers, registering identity and verifying it, as well as ongoing DD on the purpose of the relationship.
  - Note the prohibition on ‘anonymous accounts’ also needs to be overcome

• The obligation is risk based, so varies in its extent, with the risk posed; and enables focusing of resources on the greatest risks

• The requirement to undertake DD crystallises when there is a ‘business relationship’ or an occasional transaction exceeding a given threshold.

Compliance with legal obligations

• In practice, new providers have addressed this in a number of ways:
  - Lowest risk:
    - Allowing money to enter the system, but not to leave it without verification, and argue that a threshold of transactions must be passed before a business relationship can be said to have been established.
    - This is consistent with the approach of the EU 3rd ML Directive to simplified DD
  - Low risk:
    - Relying on verification undertaken by third party financial institutions such credit card issuers; such an approach is used by PayPal, and other PSP’s
  - Low to Medium risk:
    - Where available, use of electronic data to confirm identity or reliance on third parties to undertake face-to-face DD, such as high street agents
The risk of ML in practice

• The following are generalisations for low value payment products
• Risks:
  – The greatest risk lies with fraudulent or complicit merchants who would receive criminal funds masquerading as legitimate payments
  – The most prevalent typology for online payments relates to funding fraud, introducing fraudulent funds by funding with stolen credit cards
  – The risk of conventional money laundering is low, as the values transacted are low, and introducing large amounts of criminal funds will risk discovery in a number of ways
  – With money transfer products, the risk is increased and tighter control of transaction limits is needed, as is more intelligent monitoring
  – Use of airtime as a proxy for cash may pose a risk

Example approach

• Agree a fixed cumulative transaction limit before which DD is required – including requisite legal interpretation
  – If necessary allow money to enter but not exit the system before DD
• Identify vulnerabilities in the system thoroughly; then put in place limits and controls to mitigate the risks or scenarios. Then repeat!
• Explore what is conventionally regarded as verification of identity for the given jurisdiction and for law enforcement officials, with a view to using available data to compensate for data that is absent
  – Telephone voice call related information
  – Geographic data

Case study: E-money ML Guidance

• The UK regime was conventional in requiring up front verification of ID where a business relationship was created
  – In 2003 Officials accepted that by limiting turnover, and preventing funds from leaving the system, verification could be postponed, and transactions could be regarded as occasional (a UK legal anomaly)
  – In 2005 This approach was adopted by the EU Commission, and two means of undertaking Simplified DD were created:
    – Non reloadable products; a purse limit of €150 was adopted
    – Reloadable products, an annual turnover of €2500 and annual redemption (cash out) of €1000. Verification would be required to exceed these limits
• Industry guidance requires monitoring to prevent abuse through the purchase of multiple purses
  – Reliance on third parties through the micro-deposit processes was accepted into Guidance in 2005
  – The 2008 Guidance introduced the parameter of ‘time’ into the Guidance, giving weight in DD processes to transaction history
  – In 2009 the non reloadable limit was increased to €250 in the second EU E-money Directive.
  – Current discussions:
    – Can the electronic footprint of users, established over time, be used as a contributor to DD?
    – Can informal means of verification through personal relationships be used as means if verifying ID? This is particularly valuable where cash loading is involved.

Case study: E-money ML Guidance

• This has been accompanied by bimonthly typology exercises
• It has required ongoing engagement with law enforcement and regulatory officials
• Industry’s paramount concern is ensuring the products do not become vulnerable to ML
Counter terrorist financing

- With ML, the focus is on the origin of the funds, and the customer, whereas with CTF, the risk is in the use of the funds by the beneficiary
- Where CTF originates in criminal funds, then AML processes should contribute to its identification and reporting
- Where CTF originates in legitimate income, then industry is dependent on additional intelligence or typologies in order to identify and report suspicions
- Once intelligence is available, service providers can both monitor and prevent further activity

A note on the transfer of airtime

- The purchase of airtime and its transfer to others is not currently regulated under ML legislation
- Abuse of this functionality could result in pressure for regulation or a reduction in functionality
- Providers already adopt good fraud prevention systems, reducing ML risk, these can further evolve as needed to address new risks

Summary

- The main compliance challenge for mobile payment providers is undertaking consumer due diligence in an effective manner
- The solution will need to address both legal obligations and money laundering risk
- There are good precedents in the payments sector for resolving such challenges
- Industry will need to create a robust AML regime in order to deter would-be criminals

Thank You

Thaer.Sabri@e-ma.org
M +44 797 111 2066