Who carries the can?

Indirect Access to Payment Systems: The Implications of Liability

A White Paper from the Emerging Payments Association 2017
in association with the Payments Strategy Forum at the PSR

emergingpayments.org **#PayTech**

APS financial

SCOM financial services compliance

Paysafe

Foreword

Making a mistake in the armed forces used to be punished by 'carrying the can'. The can contained beer obtained and paid for by the miscreant at the local bar.

But in the rapidly evolving fintech arena, it is too often unclear who carries the can when a regulation is contravened, especially when there are so many different business models used in fintech. And it can be a pretty costly can – contravening money laundering regulations can incur fines for both for the company and responsible individuals such as the MLRO; or in some cases, imprisonment.

So when faced with such opaqueness, potential punishments and the associated commercial fall out, executives from regulated entities such as banks may well choose the path with least risk, rather than the right path.

To help reduce this opaqueness, and following an approach from a sub-committee at the Payments Strategy Forum, the Emerging Payments Association (EPA) commissioned this report from Sec-Com Advisors. The Forum is keen for this report to encourage communication between parties and help the Fintech industry to grow.

We want to shine a light on the realities of the regulations and associated risks. Progress happens when there is communication, clarity and common understanding. With additional clarity, we hope that competition and innovation will be enabled. We also hope that the rules do not prevent fintech's natural evolution while they protect users and prevent criminal and terrorist acts.

Future report topics

This report heralds what the EPA hopes will be the beginning of a series of such reports to create clarity regarding payment regulations and the complex nature of payment transactions. The reports will set out to answer these questions:

1. What is the US Customer Due Diligence Regulation and what could be its impact?

2. What are the transactions mapped between regulated entities and what needs to be monitored?

3. What constitutes a 'good profile' for a fintech regulated entity?

With thanks to . . .

I wish to express my appreciation to the many people involved with producing this report. Jane Barber as the secretary of the group, has shown great insight and helped enrich its content. John Doyle, as the chairman of the group, along with Mike Smith and Dominic Thorncroft, have shared their invaluable expert views.

And Sarah Francis at Sec-Com Advisors has guided the report on its journey through numerous touchpoints at the PSR and elsewhere. She has applied her deep knowledge of the engine room of payments to create a valuable resource to help the emerging payments industry as it matures.

So who carries the can for a mistake? What does a mistake look like? How can we keep the costs of preventing and monitoring mistakes down? Who does what to minimise the chance of mistakes? And how can we promote best practice?

Read on and find out. Then go forth and innovate.

Tony Craddock

Director General, Emerging Payments Association

tony.craddock@emergingpayments.org

Indirect Access to Payment Systems
The Implications of Liability

Contents

Thank you to our Syndicate Sponsors

We are indebted to the following three companies for their financial support for this report. It enables the Emerging Payments Association to create practical, in-depth resources that can be used across the payments ecosystem to become more innovative, competitive and successful.

APS financial

APS financial is a rapidly growing bank challenger with a mission to revolutionise the UKs digital banking experience. Proving you don't need a bank to bank, APS financial have spent the last 10 years leveraging data and technology to provide SME's and consumers with a full suite of versatile banking and lending services that meet the needs of today's digital savvy customer. For more information visit: apsfinancial.co.uk

FSCom

FSCom consultants provide expert regulatory advice and compliance services to payments and e-money businesses. Our full range of compliance services enable businesses to meet their regulatory obligations, from obtaining the correct permissions to ongoing compliance advisory and support. With offices in London, Belfast and Dublin, we are one of the leading financial services compliance consultancies in the UK and Ireland.

Our client base includes a full range of businesses-types from niche providers to leading technology-driven players. FSCom's personnel have significant experience of both best practice within the industry and understanding of the regulators' expectations and requirements.

We are members of the Association of Professional Compliance Consultants and adhere to the Code of Ethics. For more information visit: fscom.co.uk

Paysafe

Paysafe provides digital payments and transaction-related solutions to businesses and consumers around the world. Paysafe makes transactions easy by enabling fast, convenient and secure ways to pay-before, pay-now and pay-later through its digital wallets, prepaid solution, payment processing and card issuing & acquiring products and services. We believe that every point of every payment should be relevant, simple and secure. With nearly two decades of experience, Paysafe is trusted by merchants and consumers in more than 200 countries and territories, to move and manage money via more than 100 payment types and 40 currencies. Paysafe offers multi-platform products with an emphasis on emerging payment technologies including mobile. Paysafe's brand portfolio includes NETELLER® and Skrill®, MeritCard, paysafecard®, payolution®, Income Access and FANS Entertainment. Paysafe Group plc shares trade on the London Stock Exchange under the symbol (PAYS.L). For more information visit: paysafe.com.

Emerging Payments Association (EPA)

The Emerging Payments Association (EPA) is a thriving community of payments professionals whose goals are to strengthen and expand the payments industry to benefit all stakeholders. Since 2004 we have been instrumental in helping to connect the eco-system, encourage innovation and profitable business growth.

We achieve this by shaping a comprehensive programme of activities for over 100 member companies with help from our independent board, which addresses key issues impacting the industry.

These include targeted events, conferences, award ceremonies, critical industry projects and lobbying activities. For more information visit: emergingpayments.org

Executive Summary

In 2015, the Payments Strategy Forum was formed to lead a process to identify, prioritise and help to deliver initiatives where it was considered necessary for the payments industry to work together to promote collaborative innovation.

Its work was educated by detriments from the wider Payments Community on issues that prevent the UK payments market from functioning in the way the PSR envisages.

Under the simplifying access to market work, one detriment highlighted that smaller and new providers, particularly payment and e-money institutions were increasingly finding it hard to access bank accounts and as a consequence the payment systems.

The lack of opportunity to access payments systems, now classed as part of the global banking trend of 'derisking', denies many small and new PSPs the opportunity to access banking and payment services.

The conclusions of this work are that, whilst the lack of bank account provision may be seen as stifling competition for new entrants into the payments market, there is no evidence that this is because of a fear of competition by the provider banks. Rather it appears that the impacts of regulation have caused the costs and complexities involved in engaging with and monitoring the activities of the new and smaller regulated entities, to become less commercial and at the same time, still with risk attached.

This paper proposes actions, which it is considered may lead to a more normalised business environment, but which will require pan-industry and regulator engagement to achieve progress:

- Updated current guidance together with supporting business and transactional, specific guidance
- Clearer guidance from regulators of 'what constitutes failure'
- Open discussion on the costs of monitoring and how to cover them
- Co-ordinated development of Best Practice Guidance on developing working relationships with the Banks and what constitutes a 'good risk profile' for the PSP type and its transactions

Introduction

A supportive government, the ability to attract highly skilled workers and a robust technology infrastructure have all contributed to the UK's, and especially London's, position as a world leader in financial services, and its modern counterpart, FinTech.

Although FinTech technically refers to all "financial technologies", it has been endowed with a wider meaning and come to represent disruptive new entrants across the financial services spectrum from startups and incubators to funds and accelerators.

FinTech is generating a revolution in the payments industry. The Governor of the Bank of England in the transcript of his speech, which was to be given in June 2016[1] wrote of

'….a reformation – a more diverse, resilient and effective system for consumers. One where large banks exist alongside new entrants who compete across the value chain'.

Whilst the intention of the Bank is clear – to create a level playing field and accelerate competition in banking, the Governor's speech recognised that:

'FinTech has the potential to affect monetary policy transmission, the safety and soundness of the firms we supervise, the resilience of the financial system, and the nature of shocks that it might face'.

The Bank sets out its key immediate actions on FinTech and, as the systemic regulator, states that it has been engaging with firms to understand better the financial stability risks that could emerge 'as banking is re-shaped'.

As might be expected, it will monitor such firms and their activities, and concludes that once they become 'systemic and risks to the real economy grow, they will come within the purview of the Bank's responsibilities for the stability of the system as a whole'.

An example of example of this is '…widening access central bank money to non-bank Payments Service Providers..."

This paper was followed in August 2016 by the final report of the Competition and Markets Authority's (CMA) retail banking market investigation[2], which concludes that older and larger banks do not have to compete hard enough for customers' business, and smaller and newer banks find it difficult to grow. The CMA conclusions were that this means that many people are paying more than they should for services and are not benefiting from new services.

The Payment Services Regulator's (PSR) Final Report– "Market review into the supply of indirect access to payment systems"[3] makes it clear that it, the FCA, Bank of England and Prudential Regulation Authority (PRA), all have an interest in access to payment systems. Whilst the PSR will take a lead on matters relating to access to payment systems for PSPs, it will 'coordinate with these other authorities, in particular on matters relating to financial crime and access to bank accounts' (Paras. 2.20 – 2.22).

The PSR also addresses the issue that access to bank accounts is driven by a complex set of factors that include financial crime regulation supervised by other UK regulators, and that addressing these concerns through the regulation of payment systems may not be the most appropriate or effective response (3.22 -3.26).

The PSR confirmed that it will monitor developments over the next 12 months, but acknowledged that some thought it should be more explicit in how it will consider whether developments are progressing satisfactorily. The indirect access monitoring will form part of its ongoing annual access and governance reporting cycle, which until recently focused on direct access only.

The Payments Strategy Forum (PSF) was created to develop the collaborative strategy for payment systems in the United Kingdom. It was announced by the PSR in Policy Statement 15/1 published in March 2015[4] and held a first meeting in October 2015.

The PSF's group on simplifying access addressed the detriment of payment service providers not being able to obtain a bank account, and thus being barred from the payment systems. Its report proposed a mapping to articulate 'the regulatory and legal responsibilities for each party … if a party accesses a payment system via another party, which of them is considered responsible across the payment end to end journey'.

To support this strand of the simplifying access to markets activity, the Emerging Payments Association agreed to commission Sec-Com Advisors to produce a report which addresses the regulatory and legal provider and participant responsibilities in indirect access arrangements, where the participant uses the bank account to make or receive payments for its customers. The report will be supplemented with a Liability maps in support of identifying and articulating regulatory responsibilities.

The review considered the many aspects of the regulators and regulations.

The regulators overseeing the chain involved in Indirect Access to Payment systems include:

PRA – Prudential Regulatory Authority (Bank of England)

FCA – Financial Conduct Authority

PSR – Payment Services Regulator

HMRC – Revenue and Customs

The Applicable Laws covering the payment services industry include:

PRA – Banking Supervision

FCA – The Electronic Money Regulations 2011

FCA – The Payment Services Regulations 2009

FCA – The Money Laundering Regulations 2007

HMRC – The Money Laundering Regulations 2007

There are many UK regulators, regulations and laws, which can impact the liability across a transaction a chain, making it too simple to assume that there is a single answer.

The overall solutions also need to recognise the impact of regulation outside of the UK on the industry. US Anti-Money Laundering Regulation require Banks within the US to be responsible for the 'Customer's Customer', and whilst this is not applicable within the UK, US regulatory reach affects those Banks with a US entity as part of their group.

Under UK and EU regulation, certain transactions need to carry greater information and this will become more explicit when the 4th Money Laundering Directive (4MLD) becomes UK law. This provides a greater technical focus on this information.

All these regulations are applicable but it cannot be said that they provide a complete picture as to why banks appear reluctant to take on new and smaller regulated companies requiring indirect access to payment systems.

There has been a great deal of focus on the areas of regulation, covered under a broad title of AML/CFT i.e.

Money Laundering Act 2007 (MLA)

Money Laundering Regulations (2007) (MLRs)

Proceeds of Crime Act 2002 (POCA)

Prevention and Suppression of Terrorism Act (The Terrorism Act 2000)

It is avoidance of AML/CFT/Sanctions Risk, which many consider to be at the heart of current issues around indirect payments access.

The impacts of bank account closure /no supply was covered in an FCA-commissioned paper from February 2016 around De-risking: managing money-laundering risk[5]

The FCA stated:

'We are aware that some banks are no longer offering financial services to entire categories of customers that they associate with higher money laundering risk'

The go onto say:

'..we are clear that effective money-laundering risk management need not result in wholesale de-risking.'

'where a bank does not believe that it can effectively manage the money-laundering risk associated with a business relationship, it should not enter into or maintain that business relationship. But the risk-based approach does not mean that banks should deal generically with whole categories of customers or potential customers'.

It is de-risking which has generated the most controversy and this consequence of risk-based decisions needs to remain the focus of attention by regulators and industry bodies as it may provide a measure of progress for action taken.

The focus on AML/CFT/Sanctions

Indirect access to payment systems, which cover a wide range of services including:

- Bank Transfers of funds, domestically and internationally
- Bacs, CHAPs and Faster Payments schemes
- Accounts provided for Safe Guarded funds
- Access to Sort Codes
- Technical Access to payment systems like Faster Payments and Bacs
- Indirect Access to Settlement Accounts for Faster Payments

Newly regulated and smaller regulated companies, particularly MSBs have been vocal to industry bodies such as AUKPI (Association of UK Payment Institutions, EMA (Electronic Money Association) and the BBA (British Bankers Association) about their inability to access the payment systems.

The MLRs, in particular, have generated a strong reaction and concern about liability. PSPs who require payment system access but who do not wish to participate directly must gain access to a Bank Account and payment services via an indirect access provider. There remains a lack of clarity about how liability and accountability is divided between IAPs and indirect PSPs.

The PSR in their Market Review of Indirect Access and the FCA in commissioning a study into reasons 'underpinning 'derisking" and the impact of these activities and the extent which AML/CFT considerations are part of this' [6] have identified as an ongoing concern, the perceived risk of compliance failures under financial crime regulation.

There is a certain fear factor, which both risk based decision making and the goal of 'managing risk' can engender. The FATF statement on derisking, 23 October 2015[7] states:

'Supervisors should also ensure that financial institutions are taking a risk-based approach to implementing AML/CFT measures, without prejudice to rules-based measures such as targeted financial sanctions. Implementation by financial institutions should be aimed at managing (not avoiding) risks.

Given the imposed standard of a risk based approach, when IAPs agree to work with indirect PSPs, they are essentially making a judgment call based upon the indirect PSPs' ability to determine and manage AML/CTF risk with appropriate measures. This may create a perception of greater liability and risk.

AML/CFT/Sanctions – The regulation and the guidance

The regulations referenced within this report are:

The Money Laundering Regulations 2007 (MLRs)

The Proceeds of Crime Act 2002 (POCA)

The Terrorism Act 2000

These three pieces of regulation work together to form AML/CFT/Sanctions regulations, within the financial sector and are regulated by the FCA and HMRC.

The Proceeds of Crime Act Section 7 Money Laundering Offences include a within Section 330 and 331 offences with are directly focused upon the regulated section:

330 Failure to disclose: regulated sector

331 Failure to disclose: nominated officer in the regulated sector.

Offences under the AML/CFT/Sanctions regulations can lead to unlimited fines and in extreme cases imprisonment.

The MLRs set out the expectations which apply to IAPs and their relationship with indirect PSPs and have provided the detail that will be utilised in the Liability Maps.

In simple terms, MLRs impose obligations on firms and individuals in the regulated sector (that is, financial institutions, accountants, estate agents, casinos and, in some circumstances, lawyers) in relation to customer due diligence, monitoring of customers, record keeping, risk assessment and training. The obligations are intended to prevent such firms from being used for money laundering. If a firm or individual fails to comply with these requirements, criminal sanctions apply.

The area of regulation which carries the most focus for the Liability Map is contained within Part 2 – Customer Due Diligence.

A great deal of focus is placed upon the initial part of Customer Due Diligence[9]:-

5. “Customer due diligence measures” means-

(a) identifying the customer and verifying the customer’s identity on the basis of documents, data or information obtained from a reliable and independent source;

(b) identifying, where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures, on a risk-sensitive basis, to verify his identity so that the relevant person is satisfied that he knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement; and

(c) obtaining information on the purpose and intended nature of the business relationship.

Often mistaken under simple terminology like KYC and KYB, there are complexities to this regulation not least:

'on a risk-sensitive basis, to verify his identify so that the relevant person is satisfied that [he] knows who the beneficial owner is'

Complexity is introduced with, for example, the words 'risk-sensitive basis', which is added to by the term 'beneficial owner', which can mean something as relatively simple as 25% ownership. However, the regulation also states that 'as respects a body corporate,[the beneficial] otherwise exercises control over the management of the body'.

The concept of customer due diligence goes beyond what can be considered as KYC/KYB and includes Ongoing Monitoring:

Ongoing monitoring

8.—(1) A relevant person must conduct ongoing monitoring of a business relationship.

(2) "Ongoing monitoring" of a business relationship means -

(a) scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the relevant person's knowledge of the customer, his business and risk profile; and

(b) keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up-to-date.

(3) Regulation 7(3) applies to the duty to conduct ongoing monitoring under paragraph (1) as it applies to customer due diligence measures.

It should also be considered that those entities in the regulated sector fall under the need for enhanced due diligence:

Enhanced customer due diligence and ongoing monitoring

14.—(1) A relevant person must apply on a risk-sensitive basis enhanced customer due diligence measures and enhanced ongoing monitoring—

(a) in accordance with paragraphs (2) to (4);

(b) in any other situation which by its nature can present a higher risk of money laundering or terrorist financing.

There is considerable guidance available from the JMSLG (10) – within that guidance it sums up the overall focus of the MLR as:

'To apply Customer Due Diligence (CDD) measures to identify/verify customers and

To understand the nature and purpose of the proposed relationship

To maintain appropriate systems and controls for AML/CTF purposes

To monitor customer transactions and activities

To report suspicious activity, both internally and, if appropriate, externally

To keep appropriate records, and train staff

To comply with the UK financial sanctions regime'

A meaning of a 'risk based approach' is covered in detail but is summed up as:

'To assist the overall objective to prevent money laundering and terrorist financing, a risk-based approach:

- recognises that the money laundering/terrorist financing threat to firms varies across customers, jurisdictions, products and delivery channels;
- allows management to differentiate between their customers in a way that matches the risk in their particular business;
- allows senior management to apply its own approach to the firm's procedures, systems and controls, and arrangements in particular circumstances; and
- helps to produce a more cost effective system.'

It can be questioned to what extent is understood, or indeed is made clear by the FCA what failure could mean. For example, within the 2014 revised version of Part I over JMSLG guidance, it states:

'The appropriate approach in any given case is ultimately a question of judgement by senior management, in the context of the risks they consider the firm faces. The then FSA indicated in a letter to the chairman of JMLSG that:

"… If a firm demonstrates that it has put in place an effective system of controls that identifies and mitigates its money laundering risk, then [enforcement] action [by the FSA] is very unlikely."

"… [The FSA] recognise[s] that any regime that is risk-based cannot be a zero failure regime. [The FSA] appreciate[s] the importance of a non-zero failure regime; not least because a 100% standard will not be cost effective and will damage innovation, competition and legitimate commercial success."

The reference to the FSA and the fact that the link provided within the guidance no longer works provides an indication that this may no longer be a relevant statement.

The speed at which the FinTech industry is developing, together with the regulatory developments on APIs supports the need for an update on the guidance provided both by the FCA and the JMSLG. A perception of considerable negative attention including fines will contribute to Banks' overall risk assessment when producing industry risk profiles.

As the FinTech industry grows in complexity, it is also increasingly hard to label what type of entity does what. Whilst there is specific guidance within the JMSLG, which refers to interaction with MSBs (Money Service Businesses) many aspects of regulated companies identified as electronic money institutions (EMI), or payments institutions (PIs) under the regulations, carry on business that display the same risks, including cash deposits and banking agency arrangements.

Although there is guidance within the JMSLG covering E-Money issuers, this is targeted towards their interaction with customers.

It is clear there is a government intention to promote a 'level playing field' in terms of competition and access to payment systems for PSPs. To achieve this in practical terms remains complex.

The banks have a need to offer services that deliver a commercial return. To provide services to smaller companies, which requires a high level of resource to maintain effective compliance standards, may not deliver this.

The guidance available for PSPs looking to access payment systems indirectly, and for IAPs looking to offer access, is sparse and the FCA's opinion as quoted within the JMSLG is out of date.

The FCA Handbook dated as of 1st March 2016 – has this to say about the enforcement of Money Laundering Regulations (11):

'EG 19.14.601 The FCA will adopt a risk-based approach to its enforcement of the Money Laundering Regulations. Failures in anti-money laundering controls will not automatically result in disciplinary sanctions, although enforcement action is more likely where a firm has not taken adequate steps to identify its money laundering risks or put in place appropriate controls to mitigate those risks, and failed to take steps to ensure that controls are being effectively implemented.'

The Handbook also states with regards to the FCA imposition of penalties:

'EG 19.15.501 …. The FCA may not impose a penalty where there are reasonable grounds for it to be satisfied that the subject of the action tool all reasonable steps and exercised all due diligence to ensure that the relevant requirement of the Money Laundering Regulations would be met. In deciding whether a person has failed to comply with a requirement of the Money Laundering Regulations, the FCA must consider whether he followed any relevant guidance, which was issued by a supervisory authority or other appropriate body; approved by the Treasury; and published in a manner approved by the Treasury. The Joint Money Laundering Steering Group Guidance satisfies this requirement.'

Any guidance produced, by its nature needs to be non-prescriptive i.e. not a formula to follow for success. Banks' own internal risk evaluations are a part of their intellectual property in terms of their ability to compete for business.

A risk-based approach is key to applying these regulations and is the favoured governmental approach.

The terms of the Action Plan for anti-money laundering and counter-terrorist finance(12) make clear that for the foreseeable future a risk based approach will be that expected of regulated entities.

The Ministerial Foreword states:

'.. to reform the supervisory regime and ensure that those few companies who facilitate or enable money laundering are brought to task. The Government wants to ensure a risk-based approach to tackling money laundering and terrorist finance. We expect the banks and other firms subject to the Money Laundering Regulations to take a proportionate approach, focusing their efforts on the highest risks, without troubling low risk clients with unnecessary red-tape. We will continue to maintain our strong regulatory regime to ensure that our financial services industry is the best regulated in the world.'

This should be balanced by recognising the fear factor, which both risk based decision making and the goal of 'managing risk' can engender. The FATF statement on derisking, 23 October 2015 states:

'Supervisors should also ensure that financial institutions are taking a risk-based approach to implementing AML/CFT measures, without prejudice to rules-based measures such as targeted financial sanctions. Implementation by financial institutions should be aimed at managing (not avoiding) risks.

Given the imposed standard of a risk based approach when IAPs agree to work with PSPs they are essentially making a judgment call based upon the PSPs' ability to determine and manage AML/CTF risk with appropriate measures. This assists in creating a perception of greater liability and risk.

The Liability scenarios would appear to support the concern that it is a fear of failure by the IAPs of their overall compliance monitoring capabilities, which is causing reluctance to meet the needs of smaller or newly regulated companies.

This also does not take into account the costs of such systems and monitoring – there are significant resources required to meet the compliance needs of such companies. For smaller and new companies cost may be a significant factor.

The 4th Money Laundering Directive is proposed to be implemented into UK law by June 2017. There are measures within the Directive that may contribute to clarity and yet at the same time add to the overall complexity of indirect access provision.

The measures which are like to have an impact include:

- Provide a regulatory framework for virtual currency exchange platforms
- Enable FIUs and competent authorities to identify holders of bank and payment accounts.
- Harmonise the EU approach towards high-risk third countries
- Improve Transparency: new rules on access to beneficial ownership information

The implementation of 4MLD will lead to an up date to the JMLSG. This could present an opportunity also to provide more specific guidance for the indirect access of payment systems by regulated entities.

The Liabilities

In order to provide basic liability mapping, this report has focused purely on the regulation and the implications and risk judgments called for within those regulations, rather than utilising the available guidance referred to earlier in this report.

The "Core Regulations" utilised in these maps are:

The Money Laundering Regulations 2007 (MLRs)

The Proceeds of Crime Act 2002 (POCA)

Terrorism Act 2000 (TA 2000)

The concept of liability is flexible and can have many meanings including financial, legal and regulatory.

This document uses liability to describe which areas of regulation the IAPs carry responsibility for and which party carries the risk for failure to meet.

As the regulation calls for risk sensitivity and risk profiling with the associated judgment calls, there is no simple 2+2=4 equation.

The concern voiced within the PSR Market review into the supply of indirect access to payment systems is that:

'Industry responses to financial crime regulation: The perceived risk of compliance failures under financial crime regulation influences the behaviour of ISPs'

Failures could result in unlimited fines and even imprisonment of individual employees – ultimately the perceived liability. The FCA has published rules for making the Banking sector more accountable which have a big impact on the individual liability of Senior Managers and individuals (13):

- **The Senior Managers Regime** focuses on individuals who hold key roles and responsibilities in relevant firms. Preparations for the new regime will involve allocating and mapping out responsibilities and preparing Statements of Responsibilities for individuals carrying out Senior Management Functions (SMFs). While individuals who fall under this regime will continue to be pre-approved by regulators, firms will also be legally required to ensure that they have procedures in place to assess their fitness and propriety before applying for approval and at least annually afterwards.
- **The Certification Regime** applies to other staff who could pose a risk of significant harm to the firm or any of its customers (for example, staff who give investment advice or submit to benchmarks). These staff will not be pre-approved by regulators and firms' preparations will need to include putting in place procedures for assessing for themselves the fitness and propriety of staff, for which they will be accountable to the regulators. These preparations will be important not only when recruiting for roles that come under the Certification Regime but when reassessing each year the fitness and propriety of staff who are subject to the regime.
- **The Conduct Rules** set out a basic standard for behaviour that all those covered by the new regimes will be expected meet. Firms' preparations will need to include ensuring that staff who will be subject to the new rules are aware of the conduct rules and how they apply to them. Individuals subject to either the SMR or the Certification Regime will be subject to Conduct Rules from the commencement of the new regime on 7th March 2016, while firms will have a year after commencement to prepare for the wider application of the Conduct Rules to other staff.

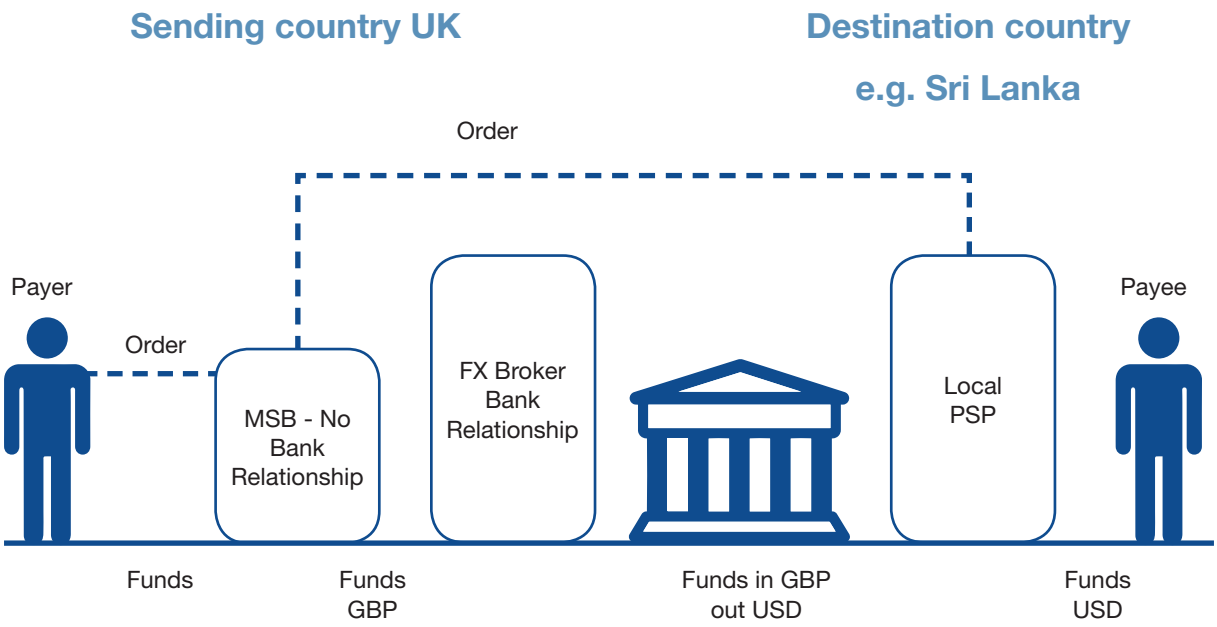
To introduce a level of context for consideration a series of scenarios has been mapped to show both successful and failed compliance measures.

It should however be noted that even with successful compliance measures there can be levels of liability and risk outside of a Bank's regulatory appetite, the consequences of which carry a commercial impact i.e. reputational or negative publicity.

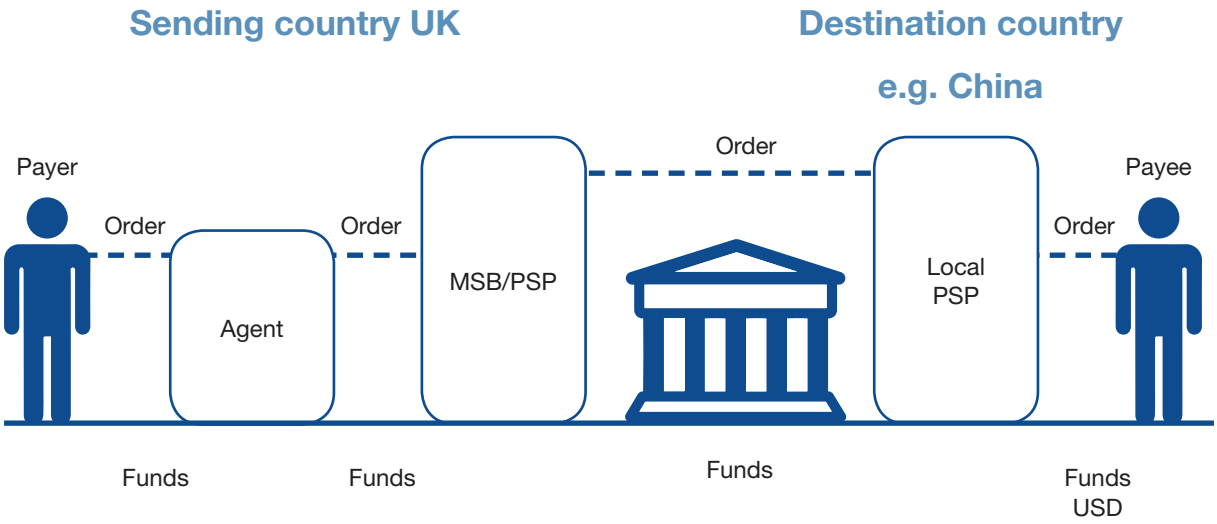
There are complex transaction arrangements that can be part of these relationships and it should not be underestimated just what is involved in developing profiles and monitoring systems.

Many transactions that are undertaken are between MSB, Forex Brokers and PI's and their equivalent in other countries and regulatory environments. Often individual transactions are not available to the banks view and funds are netted off or sent in bulk.

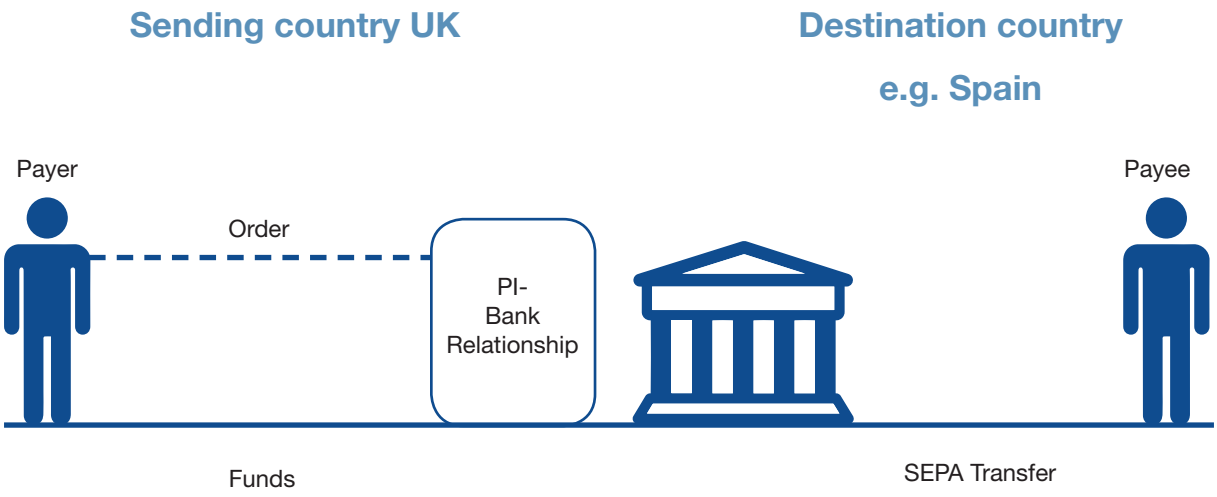
A Forex Broker for instance:



An MSB:



A PI with the simplest of transactions enabling the bank to see all transactional information:



As the liability maps are developed, consideration should be given to the situations where less transactional information requires more 'trust' and understanding of the regulated PSPs systems and processes.

Liability Map and Liability Scenarios for Agency Banking

Indirect Payment Service Provider Offering Agency Banking

Offers alternative Banking facilities to Consumers and Business, utilising a Bank Agency arrangement with an IAP.

IAP Services Utilised

Sort Codes and IBAN Numbers. Cash Deposits, Direct Debit facilities, Wire Transfers, BACS, CHAPS, SEPA transfers, Safe Guarded Consumer Funds Accounts, Currency Accounts.

PSP Regulatory Liability and Responsibility

AML/CFT - Customer Due Diligence, Enhanced Due Diligence, Ongoing Monitoring, Disclosure and Reporting.

Applied by the PSPs to their customers, consumers and business

Liability – Unlimited Fines, Imprisonment.

IAP Services Utilised

Sort Codes and IBAN Numbers. Cash Deposits, Direct Debit facilities, Wire Transfers, BACS, CHAPS, SEPA transfers, Safe Guarded Consumer Funds Accounts, Currency Accounts.

AP Risk Consideration

1. What is the regulatory structure applicable to this business?
2. Does this business fall within the IAP's risk appetite?
3. How complex is the business structure and is 'understandable' within our risk profiles?
4. Do we have a clear understanding of what constitutes 'good and bad' profiles for this type of company and how to monitor them?
5. How robust and experienced is their Management Team?
6. How strong is their Funding / Financial Backing?
7. Value and Volume – does their business / business plan provide a commercial return on the requirement resources needed for compliance monitoring.

Liability Scenario 1 – Agency Banking

This represents a scenario where the IAPs AML/CFT/Sanctions Customer Due Diligence, Enhanced Due Diligence and Ongoing Monitoring have failed. Essentially a realisation of the IAPs fears.

Indirect Payment Service Provider Offering Agency Banking

Offers alternative Banking facilities to Consumers and Business, utilising a Bank Agency arrangement with an IAP.

IAP Services Utilised

Sort Codes and IBAN Numbers. Cash Deposits, Direct Debit facilities, Wire Transfers, BACS, CHAPS, SEPA transfers, Safe Guarded Consumer Funds Accounts, Currency Accounts.

Scenario

PSP is found to be offering a product to PEPs for the purposes of Tax Evasion

The IAP failed to raise any suspicions around the clients business or transactions.

There is no evidence that the IAP 'caught' or was aware of anything suspicious with their clients activities.

IAP Regulatory Liability and Responsibility

AML/CFT - Customer Due Diligence, Enhanced Due Diligence, Ongoing Monitoring, Disclosure and Reporting.

Applied by the IAP to the PSP as customers

Ultimate Liability – Unlimited Fines, Imprisonment

Liability Risk

It could be considered that the IAP had not been utilising sufficient levels of ongoing monitoring in such a case.

The IAP may at the very least be subject to investigation

Liability Scenario 2 – Agency Banking

This represents a scenario the Regulator – FCA considers that the indirect PSP has not been implementing the correct level of ongoing monitoring.

Indirect Payment Service Provider Offering Agency Banking

Offers alternative Banking facilities to Consumers and Business, utilising a Bank Agency arrangement with an IAP.

IAP Services Utilised

SSort Codes and IBAN Numbers. Cash Deposits, Direct Debit facilities, Wire Transfers, BACS, CHAPS, SEPA transfers, Safe Guarded Consumer Funds Accounts, Currency Accounts.

Scenario

PSP is fined for having an insufficient level of Customer Due Diligence / KYC in place.

No evidence of Money Laundering or Terrorist Finance activity is found.

IAP Regulatory Liability and Responsibility

AML/CFT - Customer Due Diligence, Enhanced Due Diligence, Ongoing Monitoring, Disclosure and Reporting.

Applied by the IAP to the PSP as customers

Ultimate Liability – Unlimited Fines, Imprisonment

Liability Risk

Minimal – the IAP is not required to act as a police force on behalf of the regulator.

Liability Map and Liability Scenarios for FX and or Money Remittance Services'

Indirect Payment Service Provider Offering FX and or Money Remittance

Offers Foreign Exchange and Money Remittance Services enabling consumers and businesses to by currencies and transfer money around the world.

IAP Services Utilised

Cash Deposits, Client Accounts, Corporate Accounts, CHAPS, Wire Transfer, SEPA

Transfers, Currency Accounts.

PSP Regulatory Liability and Responsibility

AML/CFT - Customer Due Diligence, Enhanced Due Diligence, Ongoing Monitoring, Disclosure and Reporting.

Applied by the PSPs to their customers, consumers and business

Liability – Unlimited Fines, Imprisonment

IAP Regulatory Liability and Responsibility

AML/CFT - Customer Due Diligence, Enhanced Due Diligence, Ongoing Monitoring, Disclosure and Reporting.

Applied by the IAP to the PSP as customers

Ultimate Liability – Unlimited Fines, Imprisonment

IAP Risk Considerations

1. What is the regulatory structure applicable to this business?
2. Does this business fall within the IAPs risk appetite?
3. Which countries are they transferring to?
4. Will this be affected by group regulation outside of the UK?
5. How complex is the business structure and is 'understandable' within our risk profiles?
6. Do we have a clear understanding of what constitutes 'good and bad' profiles for this type of company and how to monitor them?
7. How robust and experienced is their Management Team?
8. How strong is their Funding / Financial Backing?
9. Value and Volume – does their business / business plan provide a commercial return on the requirement resources needed for compliance monitoring.

Liability Scenario 1 – FX and or Money Remittance

This represents a scenario where the IAPs AML/CFT/Sanctions Customer Due Diligence, Enhanced Due Diligence and Ongoing Monitoring have failed. Essentially a realisation of the IAPs fears.

Indirect Payment Service Provider Money Remittance Services

Offers money remittance and FX. Regulated as a PI.

IAP Services Utilised

Cash Deposits, Client Accounts, Corporate Accounts, CHAPs and SEPA Transfers

Scenario

PSP is found to be involved in Laundering over £10,000,000 in money for a major Drug Ring.
The IAP systems had failed to identify any suspicious activity.
No suspicious activity reports had been filed.

IAP Regulatory Liability and Responsibility

AML/CFT - Customer Due Diligence, Enhanced Due Diligence, Ongoing Monitoring, Disclosure and Reporting.
Applied by the IAP to the PSP as customers
Ultimate Liability – Unlimited Fines, Imprisonment

Liability Risk

High Risk the IAP is found to have insufficient monitoring, lack of internal controls, reporting and training.

Fines could be significant.

Liability Scenario 2 – FX and or Money Remittance

This is the same scenario as above without the IAP compliance failure.

Indirect Payment Service Provider Money Remittance Services

Offers money remittance and FX. Regulated as a PI.

IAP Services Utilised

Cash Deposits, Client Accounts, Corporate Accounts, CHAPs and SEPA Transfers.

Scenario

PSP is found to be involved in Laundering over £10,000,000 in money for a major Drug Ring.
The IAP identified suspicious activity and the reports had been submitted in a timely fashion.

IAP Regulatory Liability and Responsibility

AML/CFT - Customer Due Diligence, Enhanced Due Diligence, Ongoing Monitoring, Disclosure and Reporting.
Applied by the IAP to the PSP as customers
Ultimate Liability – Unlimited Fines, Imprisonment

Liability Risk

The IAP – reacted according to regulation and is deemed to have in place appropriate systems, training, reporting and internal controls.

However, the investigations and co-operation with the relevant authorities carried significant costs.

Liability Map and Liability Scenarios for Access to Faster Payments

Indirect Payment Service Provider offering a Digital Wallet

Offers consumers and merchants access to a digital wallet facility with associated prepaid card.

IAP Services Utilised

IAP Services Utilised

Has technical access to Faster Payments and seeks access to a Settlement Account with the IAP.

PSP Regulatory Liability and Responsibility

AML/CFT - Customer Due Diligence, Enhanced Due Diligence, Ongoing Monitoring, Disclosure and Reporting.

Applied by the PSPs to their customers, consumers and business

Liability – Unlimited Fines, Imprisonment .

IAP Regulatory Liability and Responsibility

AML/CFT - Customer Due Diligence, Enhanced Due Diligence, Ongoing Monitoring, Disclosure and Reporting.

No individual transaction data is available. Monitoring will cover overall company due diligence.
Ultimate Liability – Unlimited Fines, Imprisonment

IAP Risk and Commercial Considerations

1. What are the financial resources of Company?
2. What history does the management team have with regulated companies?
3. What history is there of regulatory infringements if any?
4. How successful overall is their business?
5. Do they have a sound financial history?

Liability Scenario – Access to Faster Payments

Regulatory liability under such circumstances is difficult to ascertain – there is certainly a need for ongoing monitoring of the Company, changes within the company and its offerings along with changes in management.

Financial status within this set-up is of more importance and the liability is largely financial.

What can be done?

All the reports, speeches and studies published indicate there are outstanding issues which need addressing. There are challenges that IAPs face in offering a more open access to their services to indirect PSPs. Not all the challenges are purely regulatory, nor are they purely UK biased. There are indicators that steps could be taken to improve clarity, guidance and communication.

The JMSLG is considered a good vehicle with wide enough industry representation to deliver updated guidance including a specific risk approach for banks offering services to the regulated sector beyond MSBs. Guidance could be considered that specifically address the services offered, not just the types of companies to which they are offered.

PSPs seeking to utilise the services offered by IAPs need to understand what the risks are. The BBA could assist with guidelines telling PSPs what information they need to provide and how best to approach relationships in order assist IAPs with the risk management process.

This might also include guidance on what constitutes 'a good business profile' for different types of PSPs. Whether offered by a trusted third party or a working party of industry bodies this could go a long way to assisting IAPs in their risk profiling.

Any guidance published needs to provide a clearer view on how the FCA applies penalties, or what it considers as failure in indirect access service provision.

There is some encouragement from the FCA around the need for IAPs to provide access to services. Providing greater clarity around what constitutes failure and the consequences could contribute to encouraging IAPs.

It could be recognised that increased risk monitoring required for these relationships carries a cost and ways of meeting those costs between the suppliers (IAPs) and the users (PSPs) needs to be addressed.

As part of their public information provision on indirect access services, there may be a need to require Banks / IAPs to publish more information on the services they are willing to offer and to what types of PSP. This kind of openness would do much to demystify the market.

Establishment of a 'good business profile' for PSPs to generate greater understanding of the goals sought by both PSPs and IAPs. Such guidance may be published by a trusted third party in conjunction with industry bodies, or may come from an industry body.

The goal of providing a competitive market requires a workable relationship to be found between IAPs and new, smaller PSPs. Contributions to the solution include clarity, transparency, commercial agreements and up-to-date guidance from both the regulators and the regulated.

In summary this calls for:

- Updated current guidance together with supporting business and transactional, specific guidance
- Clearer guidance from regulators of 'what constitutes failure'
- Open discussion on the costs of monitoring and how to cover them
- Co-ordinated development of Best Practice Guidance on developing working relationships with the Banks and what constitutes a 'good risk profile' for the PSP type and its transaction

FSCom's Supporting Rationale

For payment and e-money institutions, the cost of complying with anti-money laundering rules represents a significant outlay, but it is a price worth paying because maintaining their authorisation status and the relationship with their banking provider is fundamental to their business success. Just this month, the FCA's head of financial crime recognised the cost of the 'big machine' and floated ideas for reducing compliance costs, such as sharing information, centralising transaction monitoring and allowing greater reliance on the customer due diligence undertaken by other firms.

These actions along with greater clarity on where the blame will fall in an enforcement action scenario could foster the involvement of more players in the market. This is one of the drivers for the inclusion in the second Payment Services Directive of the requirement for Member States to ensure access to bank accounts 'on an objective, non-discriminatory and proportionate basis'. International guidance produced this year by the Financial Action Task Force (FATF) has been clear on supervisory expectations of how payment service providers should deal with others in such correspondent relationships. What is less clear is how this is understood by the supervisors in the UK and, indeed, given their far-reaching outlook, the US. The reputational damage of being involved in an anti-money laundering or counter-terrorist financing failure, as well as any enforcement action and fine, is significant.

According to the FCA, supervisors find the steps taken to manage the risks of the vast majority of its standard-risk customers are broadly adequate. We have certainly seen excellent examples of firms investing time and resource to develop robust systems and controls, one of the benefits of which is a mutually productive relationship with banking partners where both parties feel reasonably confident that they are meeting their respective obligations. There are undoubtedly areas where the duplication of effort can be reduced and the boundaries of liability in the chain of providers involved in the payment end to end journey can be made clearer. To that end we are pleased to support the Payment Strategy Forum in their work to clarify the regulatory and legal responsibilities for each party.

Alison Donnelly

Director and Head of Payment Services & E-money

alison.donnelly@fscom.co.uk

[1]Guidance for a risk-based approach: money or value transfer services, February 2016 and FATF guidance: correspondent banking services, October 2016

References

1 http://www.bankofengland.co.uk/publications/Documents/speeches/2016/speech914.pdf

2 https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf

3 https://www.psr.org.uk/psr-publications/market-reviews/MR1513-final-report-supply-of-indirect-access-payment-systems

4 https://www.psr.org.uk/sites/default/files/media/PDF/psr-publications-consultations-psr-ps-15.1.pdf

5 https://www.fca.org.uk/print/firms/money-laundering/derisking-managing-risk

6 https://www.fca.org.uk/publication/research/drivers-impacts-of-derisking.pdf

7 http://www.fatf-gafi.org/documents/news/rba-and-de-risking.html

8 http://www.legislation.gov.uk/ukpga/2002/29/part/7

9 http://www.legislation.gov.uk/uksi/2007/2157/part/2/made

10 www.jmlsg.org.uk/download/9803

11 https://www.handbook.fca.org.uk/handbook/EG/19/14.html?date=2016-07-03

12 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/517992/6-2118-Action_Plan_for_Anti-Money_Laundering__web_.pdf

13 https://www.fca.org.uk/news/press-releases/fca-publishes-final-rules-make-those-banking-sector-more-accountable

Appendix 1 – Proceeds of Crime 2002 Section 7

Part 7

Money Laundering

Offences

327 Concealing etc.

(1) A person commits an offence if he—

(a) conceals criminal property;

(b) disguises criminal property;

(c) converts criminal property;

(d) transfers criminal property;

(e) removes criminal property from England and Wales or from Scotland or from Northern Ireland.

(2) But a person does not commit such an offence if—

(a) he makes an authorised disclosure under section 338 and (if the disclosure is made before he does the act mentioned in subsection (1)) he has the appropriate consent;

(b) he intended to make such a disclosure but had a reasonable excuse for not doing so;

(c) the act he does is done in carrying out a function he has relating to the enforcement of any provision of this Act or of any other enactment relating to criminal conduct or benefit from criminal conduct.

(3) Concealing or disguising criminal property includes concealing or disguising its nature, source, location, disposition, movement or ownership or any rights with respect to it.

328 Arrangements

(1) A person commits an offence if he enters into or becomes concerned in an arrangement which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person.

(2) But a person does not commit such an offence if—

(a) he makes an authorised disclosure under section 338 and (if the disclosure is made before he does the act mentioned in subsection (1)) he has the appropriate consent;

(b) he intended to make such a disclosure but had a reasonable excuse for not doing so;

(c) the act he does is done in carrying out a function he has relating to the enforcement of any provision of this Act or of any other enactment relating to criminal conduct or benefit from criminal conduct.

329 Acquisition, use and possession

(1) A person commits an offence if he—

(a) acquires criminal property;

(b) uses criminal property;

(c) has possession of criminal property.

(2) But a person does not commit such an offence if—

(a) he makes an authorised disclosure under section 338 and (if the disclosure is made before he does the act mentioned in subsection (1)) he has the appropriate consent;

(b) he intended to make such a disclosure but had a reasonable excuse for not doing so;

(c) he acquired or used or had possession of the property for adequate consideration;

(d) the act he does is done in carrying out a function he has relating to the enforcement of any provision of this Act or of any other enactment relating to criminal conduct or benefit from criminal conduct.

(3) For the purposes of this section—

(a) a person acquires property for inadequate consideration if the value of the consideration is significantly less than the value of the property;

(b) a person uses or has possession of property for inadequate consideration if the value of the consideration is significantly less than the value of the use or possession;

(c) the provision by a person of goods or services which he knows or suspects may help another to carry out criminal conduct is not consideration.

330 Failure to disclose: regulated sector

(1) A person commits an offence if each of the following three conditions is satisfied.

(2) The first condition is that he—

(a) knows or suspects, or

(b) has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering.

(3) The second condition is that the information or other matter—

(a) on which his knowledge or suspicion is based, or

(b) which gives reasonable grounds for such knowledge or suspicion, came to him in the course of a business in the regulated sector.

(4) The third condition is that he does not make the required disclosure as soon as is practicable after the information or other matter comes to him.

(5) The required disclosure is a disclosure of the information or other matter—

(a) to a nominated officer or a person authorised for the purposes of this Part by the Director General of the National Criminal Intelligence Service;

(b) in the form and manner (if any) prescribed for the purposes of this subsection by order under section 339.

(6) But a person does not commit an offence under this section if—

(a) he has a reasonable excuse for not disclosing the information or other matter;

(b) he is a professional legal adviser and the information or other matter came to him in privileged circumstances;

(c) subsection (7) applies to him.

(7) This subsection applies to a person if—

(a) he does not know or suspect that another person is engaged in money laundering, and

(b) he has not been provided by his employer with such training as is specified by the Secretary of State by order for the purposes of this section.

(8) In deciding whether a person committed an offence under this section the court must consider whether he followed any relevant guidance which was at the time concerned—

(a) issued by a supervisory authority or any other appropriate body,

(b) approved by the Treasury, and

(c) published in a manner it approved as appropriate in its opinion to bring the guidance to the attention of persons likely to be affected by it.

(9) A disclosure to a nominated officer is a disclosure which—

(a) is made to a person nominated by the alleged offender's employer to receive disclosures under this section, and

(b) is made in the course of the alleged offender's employment and in accordance with the procedure established by the employer for the purpose.

(10) Information or other matter comes to a professional legal adviser in privileged circumstances if it is communicated or given to him—

(a) by (or by a representative of) a client of his in connection with the giving by the adviser of legal advice to the client,

(b) by (or by a representative of) a person seeking legal advice from the adviser, or

(c) by a person in connection with legal proceedings or contemplated legal proceedings.

(11) But subsection (10) does not apply to information or other matter which is communicated or given with the intention of furthering a criminal purpose.

(12) Schedule 9 has effect for the purpose of determining what is—

(a) a business in the regulated sector;

(b) a supervisory authority.

(13) An appropriate body is any body which regulates or is representative of any trade, profession, business or employment carried on by the alleged offender.

331 Failure to disclose: nominated officers in the regulated sector

(1) A person nominated to receive disclosures under section 330 commits an offence if the conditions in subsections (2) to (4) are satisfied.

(2) The first condition is that he—

(a) knows or suspects, or

(b) has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering.

(3) The second condition is that the information or other matter—

(a) on which his knowledge or suspicion is based, or

(b) which gives reasonable grounds for such knowledge or suspicion, came to him in consequence of a disclosure made under section 330.

(4) The third condition is that he does not make the required disclosure as soon as is practicable after the information or other matter comes to him.

(5) The required disclosure is a disclosure of the information or other matter—

(a) to a person authorised for the purposes of this Part by the Director General of the National Criminal Intelligence Service;

(b) in the form and manner (if any) prescribed for the purposes of this subsection by order under section 339.

(6) But a person does not commit an offence under this section if he has a reasonable excuse for not disclosing the information or other matter.

(7) In deciding whether a person committed an offence under this section the court must consider whether he followed any relevant guidance which was at the time concerned—

(a) issued by a supervisory authority or any other appropriate body,

(b) approved by the Treasury, and

(c) published in a manner it approved as appropriate in its opinion to bring the guidance to the attention of persons likely to be affected by it.

(8) Schedule 9 has effect for the purpose of determining what is a supervisory authority.

(9) An appropriate body is a body which regulates or is representative of a trade, profession, business or employment.

332 Failure to disclose: other nominated officers

(1) A person nominated to receive disclosures under section 337 or 338 commits an offence if the conditions in subsections (2) to (4) are satisfied.

(2) The first condition is that he knows or suspects that another person is engaged in money laundering.

(3) The second condition is that the information or other matter on which his knowledge or suspicion is based came to him in consequence of a disclosure made under section 337 or 338.

(4) The third condition is that he does not make the required disclosure as soon as is practicable after the information or other matter comes to him.

(5) The required disclosure is a disclosure of the information or other matter—

(a) to a person authorised for the purposes of this Part by the Director General of the National Criminal Intelligence Service;

(b) in the form and manner (if any) prescribed for the purposes of this subsection by order under section 339.

(6) But a person does not commit an offence under this section if he has a reasonable excuse for not disclosing the information or other matter.

333 Tipping off

(1) A person commits an offence if—

(a) he knows or suspects that a disclosure falling within section 337 or 338 has been made, and

(b) he makes a disclosure which is likely to prejudice any investigation which might be conducted following the disclosure referred to in paragraph (a).

(2) But a person does not commit an offence under subsection (1) if—

(a) he did not know or suspect that the disclosure was likely to be prejudicial as mentioned in subsection (1);

(b) the disclosure is made in carrying out a function he has relating to the enforcement of any provision of this Act or of any other enactment relating to criminal conduct or benefit from criminal conduct;

(c) he is a professional legal adviser and the disclosure falls within subsection (3).

(3) A disclosure falls within this subsection if it is a disclosure—

(a) to (or to a representative of) a client of the professional legal adviser in connection with the giving by the adviser of legal advice to the client, or

(b) to any person in connection with legal proceedings or contemplated legal proceedings.

(4) But a disclosure does not fall within subsection (3) if it is made with the intention of furthering a criminal purpose.

334 Penalties

(1) A person guilty of an offence under section 327, 328 or 329 is liable—

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both, or

(b) on conviction on indictment, to imprisonment for a term not exceeding 14 years or to a fine or to both.

(2) A person guilty of an offence under section 330, 331, 332 or 333 is liable—

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both, or

(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

Consent

335 Appropriate consent

(1) The appropriate consent is—

(a) the consent of a nominated officer to do a prohibited act if an authorised disclosure is made to the nominated officer;

(b) the consent of a constable to do a prohibited act if an authorised disclosure is made to a constable;

(c) the consent of a customs officer to do a prohibited act if an authorised disclosure is made to a customs officer.

(2) A person must be treated as having the appropriate consent if—

(a) he makes an authorised disclosure to a constable or a customs officer, and

(b) the condition in subsection (3) or the condition in subsection (4) is satisfied.

(3) The condition is that before the end of the notice period he does not receive notice from a constable or customs officer that consent to the doing of the act is refused.

(4) The condition is that—

(a) before the end of the notice period he receives notice from a constable or customs officer that consent to the doing of the act is refused, and

(b) the moratorium period has expired.

(5) The notice period is the period of seven working days starting with the first working day after the person makes the disclosure.

(6) The moratorium period is the period of 31 days starting with the day on which the person receives notice that consent to the doing of the act is refused.

(7) A working day is a day other than a Saturday, a Sunday, Christmas Day, Good Friday or a day which is a bank holiday under the Banking and Financial Dealings Act 1971 (c. 80) in the part of the United Kingdom in which the person is when he makes the disclosure.

(8) References to a prohibited act are to an act mentioned in section 327(1), 328(1) or 329(1) (as the case may be).

(9) A nominated officer is a person nominated to receive disclosures under section 338.

(10) Subsections (1) to (4) apply for the purposes of this Part.

336 Nominated officer: consent

(1) A nominated officer must not give the appropriate consent to the doing of a prohibited act unless the condition in subsection (2), the condition in subsection (3) or the condition in subsection (4) is satisfied.

(2) The condition is that—

(a) he makes a disclosure that property is criminal property to a person authorised for the purposes of this Part by the Director General of the National Criminal Intelligence Service, and

(b) such a person gives consent to the doing of the act.

(3) The condition is that—

(a) he makes a disclosure that property is criminal property to a person authorised for the purposes of this Part by the Director General of the National Criminal Intelligence Service, and

(b) before the end of the notice period he does not receive notice from such a person that consent to the doing of the act is refused.

(4) The condition is that—

(a) he makes a disclosure that property is criminal property to a person authorised for the purposes of this Part by the Director General of the National Criminal Intelligence Service,

(b) before the end of the notice period he receives notice from such a person that consent to the doing of the act is refused, and

(c) the moratorium period has expired.

(5) A person who is a nominated officer commits an offence if—

(a) he gives consent to a prohibited act in circumstances where none of the conditions in subsections (2), (3) and (4) is satisfied, and

(b) he knows or suspects that the act is a prohibited act.

(6) A person guilty of such an offence is liable—

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both, or

(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

(7) The notice period is the period of seven working days starting with the first working day after the nominated officer makes the disclosure.

(8) The moratorium period is the period of 31 days starting with the day on which the nominated officer is given notice that consent to the doing of the act is refused.

(9) A working day is a day other than a Saturday, a Sunday, Christmas Day, Good Friday or a day which is a bank holiday under the Banking and Financial Dealings Act 1971 (c. 80) in the part of the United Kingdom in which the nominated officer is when he gives the appropriate consent.

(10) References to a prohibited act are to an act mentioned in section 327(1), 328(1) or 329(1) (as the case may be).

(11) A nominated officer is a person nominated to receive disclosures under section 338.

Disclosures

337 Protected disclosures

(1) A disclosure which satisfies the following three conditions is not to be taken to breach any restriction on the disclosure of information (however imposed).

(2) The first condition is that the information or other matter disclosed came to the person making the disclosure (the discloser) in the course of his trade, profession, business or employment.

(3) The second condition is that the information or other matter—

(a) causes the discloser to know or suspect, or

(b) gives him reasonable grounds for knowing or suspecting, that another person is engaged in money laundering.

(4) The third condition is that the disclosure is made to a constable, a customs officer or a nominated officer as soon as is practicable after the information or other matter comes to the discloser.

(5) A disclosure to a nominated officer is a disclosure which—

(a) is made to a person nominated by the discloser's employer to receive disclosures under this section, and

(b) is made in the course of the discloser's employment and in accordance with the procedure established by the employer for the purpose.

338 Authorised disclosures

(1) For the purposes of this Part a disclosure is authorised if—

(a) it is a disclosure to a constable, a customs officer or a nominated officer by the alleged offender that property is criminal property,

(b) it is made in the form and manner (if any) prescribed for the purposes of this subsection by order under section 339, and

(c) the first or second condition set out below is satisfied.

(2) The first condition is that the disclosure is made before the alleged offender does the prohibited act.

(3) The second condition is that—

(a) the disclosure is made after the alleged offender does the prohibited act,

(b) there is a good reason for his failure to make the disclosure before he did the act, and

(c) the disclosure is made on his own initiative and as soon as it is practicable for him to make it.

(4) An authorised disclosure is not to be taken to breach any restriction on the disclosure of information (however imposed).

(5) A disclosure to a nominated officer is a disclosure which—

(a) is made to a person nominated by the alleged offender's employer to receive authorised disclosures, and

(b) is made in the course of the alleged offender's employment and in accordance with the procedure established by the employer for the purpose.

(6) References to the prohibited act are to an act mentioned in section 327(1), 328(1) or 329(1) (as the case may be).

339 Form and manner of disclosures

(1) The Secretary of State may by order prescribe the form and manner in which a disclosure under section 330, 331, 332 or 338 must be made.

(2) An order under this section may also provide that the form may include a request to the discloser to provide additional information specified in the form.

(3) The additional information must be information which is necessary to enable the person to whom the disclosure is made to decide whether to start a money laundering investigation.

(4) A disclosure made in pursuance of a request under subsection (2) is not to be taken to breach any restriction on the disclosure of information (however imposed).

(5) The discloser is the person making a disclosure mentioned in subsection (1).

(6) Money laundering investigation must be construed in accordance with section 341(4).

(7) Subsection (2) does not apply to a disclosure made to a nominated officer.

Interpretation

340 Interpretation

(1) This section applies for the purposes of this Part.

(2) Criminal conduct is conduct which—

(a) constitutes an offence in any part of the United Kingdom, or

(b) would constitute an offence in any part of the United Kingdom if it occurred there.

(3) Property is criminal property if—

(a) it constitutes a person's benefit from criminal conduct or it represents such a benefit (in whole or part and whether directly or indirectly), and

(b) the alleged offender knows or suspects that it constitutes or represents such a benefit.

(4) It is immaterial—

(a) who carried out the conduct;

(b) who benefited from it;

(c) whether the conduct occurred before or after the passing of this Act.

(5) A person benefits from conduct if he obtains property as a result of or in connection with the conduct.

(6) If a person obtains a pecuniary advantage as a result of or in connection with conduct, he is to be taken to obtain as a result of or in connection with the conduct a sum of money equal to the value of the pecuniary advantage.

(7) References to property or a pecuniary advantage obtained in connection with conduct include references to property or a pecuniary advantage obtained in both that connection and some other.

(8) If a person benefits from conduct his benefit is the property obtained as a result of or in connection with the conduct.

(9) Property is all property wherever situated and includes—

(a) money;

(b) all forms of property, real or personal, heritable or moveable;

(c) things in action and other intangible or incorporeal property.

(10) The following rules apply in relation to property—

(a) property is obtained by a person if he obtains an interest in it;

(b) references to an interest, in relation to land in England and Wales or Northern Ireland, are to any legal estate or equitable interest or power;

(c) references to an interest, in relation to land in Scotland, are to any estate, interest, servitude or other heritable right in or over land, including a heritable security;

(d) references to an interest, in relation to property other than land, include references to a right (including a right to possession).

(11) Money laundering is an act which—

(a) constitutes an offence under section 327, 328 or 329,

(b) constitutes an attempt, conspiracy or incitement to commit an offence specified in paragraph (a),

(c) constitutes aiding, abetting, counselling or procuring the commission of an offence specified in paragraph (a), or

(d) would constitute an offence specified in paragraph (a), (b) or (c) if done in the United Kingdom.

(12) For the purposes of a disclosure to a nominated officer—

(a) references to a person's employer include any body, association or organisation (including a voluntary organisation) in connection with whose activities the person exercises a function (whether or not for gain or reward), and

(b) references to employment must be construed accordingly.

(13) References to a constable include references to a person authorised for the purposes of this Part by the Director General of the National Criminal Intelligence Service.

Emerging Payments Association
Colechurch House, 1 London Bridge Walk,
London, SE1 2SX
Tel: **+44 (0)20 7378 9890**
Web: **emergingpayments.org**
Email: **info@emergingpayments.org**
@EPAssoc #PayTech