Drivers & Impacts of Derisking

A study of representative views and data in the UK, by John Howell & Co. Ltd. for the Financial Conduct Authority

David Artingstall, Nick Dove, John Howell, Michael Levi

February 2016

John Howell & Co. Ltd.
Firs House, Firs Lane
Shamley Green, Surrey GU5 0UU (UK)
Tel +44 (0)1483 890212 Fax +44 (0)1483 890213 *contact@jh-co.com*

Company No. 4500106 England and Wales

Table of Contents

TABLE OF ACRONYMS

4MLD	European Union 4th Money Laundering Directive
ACAMS	Association of Certified Anti-Money Laundering Specialists
AML	Anti-Money Laundering
ATM	Automated Teller Machine
BBA	British Bankers' Association
BIS	Department of Business, Innovation & Skills
CA	Citizens' Advice (Bureau)
CAAT	Campaign Against Arms Trade
CAF	Charities Aid Foundation
CDD	Customer Due Diligence
CFG	Charities Finance Group
CFT	Combating the Financing of Terrorism
CMA	Competition and Markets Authority
DCA	Digital Currency Association
DPA	Deferred Prosecution Agreement
EDD	Enhanced Due Diligence
EMA	E-Money Association
EMI	Electronic Money Institution
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
FinTech	Financial Technology
FIU	Financial Intelligence Unit
FOS	Financial Ombudsman Service
HMT	Her Majesty's Treasury
ID	Identification
JH&Co	John Howell & Co Ltd
JMLSG	Joint Money Laundering Steering Group
KYC	Know Your Customer
ML	Money Laundering
MOD	Ministry of Defence
MSB	Money Service Business
MTO	Money Transfer Operators
NPA	National Pawnbrokers Association
NRA	National Risk Assessment
PCA	Personal Current Account
PEP	Politically Exposed Person
PI	Payment Institution
POA	Proof of Address
POCA	Proceeds of Crime Act
POI	Proof of Identity
POS	Point of Sale
PSD	Payment Services Directive
RBA	Risk Based Approach
SAR	Suspicious Activity Report
SME	Small and Medium-sized Enterprise
TF	Terrorist Finance
UKEF/ECGD	United Kingdom Export Finance/Export Credit Guarantee Department

1 INTRODUCTION

The Financial Conduct Authority (FCA) is aware that over recent years some banks have removed bank accounts/services from customers or other relationships which they associate with higher money laundering risk. This process has been termed 'derisking' and it has been attributed to the increasing overall cost of complying with regulatory requirements. These include prudential and conduct obligations and, standards as well as the threat of enforcement action for failing to meet such obligations, particularly in relation to anti-money laundering/combating financing of terrorism (AML/CFT). However, there appear to be other factors at play too, including ethical, reputational and commercial considerations.

The FCA commissioned John Howell & Co. Ltd. (JH&Co) to undertake a short study to produce reliable evidence of the reasons underpinning derisking, the nature, scale and impact of those activities and the extent to which AML/CFT considerations are part of these reasons. While 'derisking' as a term might have grown to have possibly unfair negative connotations, including suggesting poor practice by banks, it is adopted in this report simply as convenient shorthand.

The study looked at questions posed by the FCA in four broad areas – the drivers of derisking, the exclusion costs of derisking; the costs of triage (i.e. the costs for banks of onboarding customers and costs to customers of meeting AML obligations); and mitigations of derisking programmes.

Sectors at risk from derisking highlighted by the FCA for the purposes of this study include Money Service Businesses (MSBs), charities and Financial Technology (FinTech) companies. There has also been a contraction of correspondent banking relationships. Given the role these sectors play in supporting developing economies, UK communities and businesses, derisking could be having a significant socio-economic impact.

The FCA's strategic objective is to ensure that financial markets work well so that consumers get a fair deal.

This is supported by three operational objectives[1]:

- Securing an appropriate degree of protection for consumers,
- Protecting and enhancing the integrity of the UK financial system,
- Promoting effective competition for the benefit of consumers (in markets for financial services).

In the context of financial crime, the FCA requires all authorised firms to have systems and controls in place to mitigate the risk that they might be used to commit financial crime.[2]

The FCA is the anti-money laundering supervisor of authorised firms under the Money Laundering Regulations 2007 and can take action where it finds evidence of financial crime, or a risk of it, in the sectors and markets it regulates.

[1] See FCA website, 'What we do', http://www.fca.org.uk/about/what

[2] See FCA website, 'Enforcing our rules and fighting financial crime', http://www.fca.org.uk/about/what/enforcing

The Financial Action Task Force (FATF), the international standard setter in the anti-money laundering/combating terrorist finance (AML/CFT) field, states that *'Effective action against money laundering and terrorist financing, including both preventive and law enforcement measures, is essential for securing a more transparent and stable international financial system.'* Effective systems and controls in firms can help them to detect, prevent and deter financial crime. Again according to the FATF, '*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.*'[3]

In this short study, the project team from JH&Co have interviewed an appropriate range of banks, customers and other third parties involved in order to seek evidence of the derisking phenomenon which may help shed light on the FCA's questions. A more detailed methodology is set out in Section 8 of this report.

[3] FATF statement on derisking, 23 October 2015: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-action-to-tackle-derisking.html

2 SUMMARY AND OVERVIEW

The FCA is interested in the circumstances around banks closing customers' accounts, or restricting access for new customers, over the last few years. It wishes to know more about what is driving account closure and how many customers, of which type, are affected. The FCA is also concerned as to whether 'wholesale' derisking and financial exclusion from the withdrawal of banking services is occurring, and if due consideration is being given to the merits of individual cases before a decision is made to terminate an existing account or not to grant a new account.

The FCA wishes to understand which impacted customers have faced difficulties, delays and account closures. The FCA believes these to include Small and Medium-sized Enterprises (SMEs), the FinTech and defence sectors, personal account holders (including minorities and vulnerable groups), and those who are discouraged from using the banking system.

2.1 Drivers of Derisking (See Sections 3 & 4)

Many banks told us that they needed to lower their overall risk profile, to realign their businesses and that they are paying closer attention to compliance since the global financial crisis. Further, we heard that derisking is partly a result of the higher costs of compliance and the increased amount of regulatory capital now required, and partly a response to criminal, civil and regulatory actions. These include regulatory settlements, including Deferred Prosecution Agreements (DPAs), especially those reached in response to AML/CFT failings.

There is also no doubt that banks are trying to do what they believe is expected of them under the risk based approach (RBA) to AML/CFT, in reducing the extent to which their services are abused for financial crime purposes, by on occasion exiting relationships that present too high a perceived risk of such abuse, regardless of the costs of compliance. These perceptions of risk stem from their own judgments, in part reflecting the signals emitted (or judged to be emitted) from the range of regulators and prosecutors who are salient to their institutions, and also the global rankings from the commercial agencies involved in risk judgments.

Higher compliance costs may also be reducing incentives for larger banks to maintain many interbank relationships, which previously were seen as providing extra cover or transactional options: a majority of the small and medium-sized banks surveyed reported difficulties, which in some cases have led to them cutting services to customers and to other banks.

We assess that other factors have combined with regulatory actions, higher compliance costs and perceived pressure from correspondent banks, to create a 'perfect storm' of changes which have struck banks during this decade. These include much higher capital requirements; higher liquidity thresholds and ultimately a tougher environment in which to achieve profitable relationships.

For the majority of our bank interviewees, this has resulted in a strategic review of business and functions, often in parallel with an over-arching review of compliance risk processes. In turn this has sometimes resulted in slimming down of business, resulting in many exits being driven by the assessment that relationships are 'non-core'. So we are describing a compound situation in which a range of factors may be involved in many of the exits. Ultimately, banks may feel themselves entitled to do business or not

do business with whomever they like, subject to legal (including regulatory) requirements.

Achieving the perception of legitimacy and fairness of the regulatory system requires consistency and transparency when dealing with each type of customer. Established risk-based approaches to financial crime identify the risk associated with various factors such as sector, occupation, types of business; geography and jurisdiction risk; political risk; distribution channels; and product or services that customer requires or uses. However, by contrast to some other banking risks like consumer credit loss and fraud risks, there is not yet a generally agreed quantitative assessment methodology for assessing financial crime risk and it is difficult to determine to what extent the data are sufficient for this purpose, other than to make a broad subjective assessment.

Banks vary in their ability to 'score' particular customers, depending on the bank's size, resources, geographic coverage and other factors. Decisions on what financial crime residual risks fall within acceptable parameters for a particular bank may be taken through an expression of financial crime risk appetite and/or as an output from customer risk assessment tools, using the broad risk factor categories.

Risk appetite statements often contain broad definitions of acceptable risk, such as 'minimal tolerance for residual Financial Crime risk', but we have also found examples where particular sectors are specifically mentioned. If this amounted to a complete prohibition it could be classified as 'wholesale derisking', but we have found few examples relating solely to AML/CFT issues. Reputational risk, bribery and corruption concerns and strategic business reasons also factor in to some banks ruling out the banking of certain sectors, for example the defence industry.

Outputs from customer risk assessment tools will group customers into risk categories (e.g., at the simplest level, High, Medium, Low). De-risking can also come about by setting scores from these tools above which the customer is defined to be beyond financial crime risk appetite, or to require special consideration. Although this would be regarded as 'case-by-case' derisking by the banks, it almost inevitably means that the customers identified share common characteristics, such as sector, business type and country affiliations. From the point of view of those affected by derisking, this would give the impression of a wholesale process.

However, those interviewed from banks were adamant that their institutions were doing their best to treat each customer in a fair and consistent manner. Such consistency itself is likely to produce derisking, even if it is not intended to: it is an unintended outcome of common judgments using shared criteria.

Banks have processes in place to consider keeping or exiting customer relationships on a case-by-case basis. Once a customer has been identified as being outside a bank's risk appetite, any decision to retain must be based on solid information showing that, although falling within the 'too high' risk cohort, this *particular* customer in fact poses a lower risk. In a sense it is an attempt to prove a negative and it is difficult to establish clear criteria for how this might be done.

Banks have developed techniques to differentiate risk within one particular class of customer they are obliged by law to treat as high risk, namely non-domestic Politically Exposed Persons (PEPs). Perhaps similar approaches could be applied to other commonly accepted money laundering/terrorist finance (ML/TF) high or higher risk sectors – for example, if certain types of MSBs operating in certain markets are

regarded as high risk, what characteristics, if any, might identify the 'good' from the 'bad' within that category?

Triggers for exclusion of existing or new customers usually come from reviews (which may be routine); or as a result of interpretations of general regulatory guidance, including statements from international bodies; or from particular events, including intended or unintended 'signals' during supervisory visits. A minority of such reviews identify customers suspected to be involved in financial crime, although the immediate reason for account closure or restriction can be such issues as failed background checks; failure to supply adequate and verifiable identification; fraud markers (e.g. adverse Cifas[4] traces); general credit/operational risk reasons; dormant or non-profitable accounts; and accounts not being used for the originally declared purposes (particularly when outside the bank's core business). Such events may be proxies for financial crime – criminals may fail to provide adequate identification, for example - but they are not explicit or unique ones (other, non-criminal, potential customers may also have issues with identification documentation), nor do they need to be to have that effect.

In some cases, however, banks may over-ride customer risk ratings, or apply them only to new relationships, if changes in a particular factor, for example country risk, have a significant effect on many of their customers. In others, larger banks may supply lists to smaller banks of customer types they don't wish to handle, which, irrespective of regulators' abstract statements about their not needing to know your customer's customers, may cause a 'cascade effect' of excessive caution based around a reasonable fear by the smaller banks that their own relationships with larger ones will be imperilled should they bank these sectors.

Our sections on account turnover of non-banks and of interbank relationships provide evidence, in broad terms, of clients being exited in the last 2-3 years at an accelerated rate. The single largest reason, numerically, is culling of dormant accounts, but 'higher ML/TF risk' customers have also typically been disproportionately impacted through a mixture of the focus of strategic reviews, thinly stretched compliance capacity and reduced risk appetite. For example, two large UK banks are together closing around 1,000 personal and 600 business/corporate accounts per month for 'risk appetite'-type reasons. Such closures are not readily apparent because they are dwarfed by the mass ebb and flow of accounts, and in general these banks have carried on growing numbers of accounts and customers.

Our findings are that the most consistent impacts have been in correspondent banking, where all banks report a net reduction and among MSBs (at some banks). This confirms the narrative found in much of the literature on de-risking, which has tended to focus on correspondent banking, MSBs and charities as sectors at risk[5]. We have also

[4] Cifas is a not-for-profit company working to protect businesses, charities, public bodies and individuals from financial crime. No longer an acronym, formerly the Credit Industry Fraud Avoidance Service. www.cifas.org.uk

[5] Summaries can be found in, for example, *Unintended Consequences of Anti–Money Laundering Policies for Poor Countries: A CGD Working Group Report,* Centre for Global Development, June 2015 (http://www.cgdev.org/publication/unintended-consequences-anti-money-laundering-policies-poor-countries) and *Understanding Bank De-risking and Its Effects on Financial Inclusion,* Global Center on Cooperative Security/Oxfam, November 2015 (http://www.globalcenter.org/publications/understanding-bank-de-risking-and-its-effects-on-financial-inclusion-2/). The G20 has asked for reports on both the remittance market by the World Bank

found, via the 'bank cascade', customers of small and medium-sized banks have had difficulties. In particular at those banks with foreign parents we sometimes found a large net reduction in client numbers. The outcome is an increased difficulty for foreign nationals and foreign businesses to retain UK-based accounts, or to carry out a full range of banking across currencies and jurisdictions. Some of our interviewee banks mentioned specific challenges in cross border transactions, including trade-related finance.

Responses received indicate that SMEs are more likely to be derisked than larger firms in the same sector; that the lists and methods used by smaller institutions to assess country risk may be sub-optimal; and that relationships which involve cash handling or value transfers (particularly cross-border) are seen as problematic, because of the lack of visibility of the underlying transactions to banks, including potential sanctions issues, and the perception of the inadequate quality of risk management by those offering value transfer services.

Specific sectoral concerns, which may highlight types of cutomers vulnerable to derisking, include the transfer of riskier customers, who lack bank accounts, to the Money Service Business (MSB) sector, which may have less ability to manage risk; start-ups in the FinTech sector with poorly understood business models and still-evolving systems of regulation; and the impact of the new 4th European Directive on AML/CFT (4MLD) on costs. Examples given include potentially stricter requirements on law firms' client accounts and the number of interbank relationships that need to be monitored.

2.2 The Exclusion Costs of Derisking (See Section 5)

Derisking is not generally a widespread phenomenon, but in sectors where it occurs it tends to be frequent. While this does pick up some customers with genuine financial crime issues, and perhaps others whose financial crime risks are real but undetected, all companies or individuals caught in its dragnet may suffer significant expense and inefficiency. This may lead to reduced supply and/or increase costs of goods and services that can be obtained by banks and provided by the derisked.

Defence

The defence sector has a difficult position. Financing for legitimate defence needs and legitimate defence contractors has often been overshadowed by controversies over controversial contracts and countries, creating an environment where banks fear to be conspicuous. A recent survey carried out for the industry found that banks appear unwilling to provide banking services, including letters of credit, to defence sector SMEs, particularly those involved in munitions. In the past, this had caused some SMEs to relocate overseas. Further, some cases of account closure were attributed to derisking. Dialogue between the industry and the British Bankers' Association (BBA) is now said to be improving access, and the situation is being kept under review by the defence industry via one of its leading associations.

(http://documents.worldbank.org/curated/en/2015/11/25478384/report-g20-survey-de-risking-activities-remittance-market) and correspondent banking/trade finance by the Financial Stability Board (http://www.fsb.org/2015/11/fsb-releases-report-to-g20-on-the-decline-in-correspondent-banking/)

Charities

Charities, which received £10.6bn donations in the UK in 2014, are dependent on banking facilities to collect and manage this money. A non-trivial number of charities have a religious focus or operate in geographic areas with at least some money laundering/terrorist finance (ML/TF) issues, and the recently published National Risk Assessment of Money Laundering and Terrorist Financing[6] (NRA) stated that, despite *proven* abuse being rare, the terrorist financing risks within the charitable sector are medium-high. Charities surveyed highlighted the impact of derisking on smaller charities, particularly those with activities in problematic countries, some of which now have to operate on a cash only basis, which increases their operational risks and costs.

The Charities Aid Foundation (CAF) – which helps 1,250 charities – and the Charities Finance Group (CFG) – with 2,300 members - are both concerned that there may soon be an 'avalanche' of derisking affecting smaller institutions. Although larger charitable organisations are not at risk of losing accounts, one famous name charity reported a need for advice worth at least £40k about sanction regimes, and more on complex requests for information from banks. As with businesses we contacted, charities have reported that a refusal/derisking by one bank compromises the success of approaches to other banks.

Diplomats and Foreign Students

We encountered crown and civil servants, including members of the UK diplomatic service who had served abroad (who in UK legislation are not defined as PEPs, ex *officio*) and foreign diplomats moving to the UK (defined in UK law as PEPs, ex *officio*), who had had problems obtaining bank accounts by virtue of their positions. Lack of credit history and history of recent abode also impeded access to financial services on the same terms as home-based staff.

Foreign students seeking to open accounts reported many difficulties over identification (ID) documentation and high (to them) costs of satisfying verification and Customer Due Diligence (CDD): an example being aked by banks for original documents, which had to be obtained from home countries, where the necessity of the UK requirements was questioned.

Financial Technology (FinTech)

The UK accounts for around half of European FinTech start-ups, and a 2014 report estimates the FinTech market for which companies in the UK compete to be worth £20bn. Customers turn to FinTech partly because of challenges in accessing or dissatisfaction with traditional banking services and existing bank technology. However, like all payment systems, novel payment systems are a potential vector for illegal activity and thus liable to trigger derisking decisions.

The E-Money Association (EMA) represents 44 FinTech companies, including famous names like Google and Facebook as well as start-ups. In 2012 its members had 85m customers and processed 1.3bn transactions worth €43.6bn. EMA has previously made submissions to the FCA including that its members have seen a decline of ease of access

[6] UK National Risk Assessment of Money Laundering and Terrorist Financing (HMT, HO) 2015 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf

to accounts, partly attributed to derisking policy. EMA has suggested that whilst Electronic Money Institutions and/or Payment Institutions (EMI/PIs) may be viewed as particularly risky clients by banks, refusals are often by letter with no explanation or remedial action being offered, reducing the scope for discussion. The NRA rated new payments methods (e-money) as a 'Medium' risk and digital currencies as a 'Low' risk for money laundering.

EMI/PIs include money remittance companies serving migrant workers, debit/prepaid card issuers, automated teller machine (ATM) and point of sale (POS) acquirers, and companies dealing with gambling services. These services can be seen as providing some financial solutions to underbanked groups. EMA provided three case studies where EMIs and online payment processors had been refused accounts or had accounts closed by a number of first and second tier banks. A further company which seeks to provide alternative bank services for SMEs reported difficulties obtaining assistance from one particular bank and believed that there was a blanket ban on assisting with blockchain operations. The Digital Currency Association (DCA) echoed similar concerns, which it says it has brought to government attention.

Money Transfer Operators (MTOs)

The well-publicised decision by certain banks to close a significant proportion of their Money Transfer Operator (MTO), among other MSBs, accounts in 2012-13, and subsequent legal action taken by Dahabshiil and others, brought derisking to escalating public and political attention, and highlighted concerns about a potential humanitarian catastrophe precipitated by global restrictions on remittances.

Many small MTOs (and other MSBs) now see their situation as precarious, and are being pressurised to become part of larger groups even though some believe they are more effective as independents. Some regard this as a commercial decision by banks, with AML/CFT control issues used as an excuse. A case study which explores this issue is provided in the body of report.

The NRA rates MSBs (in all guises, not just MTOs) as a 'Medium' risk for money laundering, but 'High' for terrorist finance. However, transfer of criminal funds overseas and third party payments (used by some MTOs) are highlighted as specific money laundering threats and vulnerabilities to the sector.

Financial services for the unbanked

Personal credit plays an important role in supporting those, typically on low incomes, who have difficulty managing their finances and who are unable or unwilling to access mainstream credit sources. A number of pawnbrokers and other personal credit suppliers we talked to said that small businesses and the self-employed have increasingly turned to personal credit following the 2008/9 crash and increased difficulty in accessing normal bank credit. UNITE/European Commission figures for April 2015 suggest that nine million adults in the UK do not have a bank account and one of the few options these people have to access financial services is from personal credit providers.

Pawnbrokers and home credit businesses have historically provided one alternative to those loan sharks and unscrupulous doorstep lenders whose recovery practices and

high interest rates can be catastrophic for those already vulnerable[7]. Taken together, pawnbrokers and MSBs provide up to £5bn finance in the UK, and around 10% of their outlets are in rural locations. If many of these closed, the industry argues, it could have a major effect on communities affecting around one million people, in particular by removing credit and cheque-cashing provision for many lower income groups. Wales, Northern Ireland, parts of Scotland and Cornwall would be worst affected.

A survey carried out by the National Pawnbrokers Association (NPA) in September 2015 showed that over 40% of members had had an account closed. After one bank was the first to exit relationships in the sector, two others followed. The resulting concentration has reduced competition and the NPA also believes there is a risk of independent members being forced out of the market, thus reducing consumer choice. Case studies of viable home credit businesses, with long and trouble-free banking histories, highlight sudden termination of banking facilities with no explanation or discussion. They suggest that at least part of the personal credit sector is being impacted adversely by derisking.

Quantitative Estimates of Impact

One source of data on the impact of derisking is provided by the Financial Ombudsman Service (Ombudsman Service), which reports a current case load of 20-30 complaints about account closures due to AML or personal current account (PCA) issues per week. Subject to margins of error this would imply roughly a thousand cases annually. Obtaining meaningful wider conclusions from Ombudsman Service data would require work beyond the scope of this study.

Citizens Advice (CA) assisted 3,936 clients with bank or post-office account opening from 1st October 2014 to 8th November 2015, and it has observed issues over proof of identity and lack of formal accommodation. Generally, quantification based on complaints or survey responses has been beyond the resources of this study given the need to take account under-reporting by SMEs (because of concern over reputation and lack of formal compliance cost estimation), and practical obstacles to contacting the discouraged and vulnerable groups.

2.3 The Costs of Triage (see Section 6)

Almost all the banks we have spoken to have increased spending on AML/CFT compliance, including on-boarding, monitoring and second line functions. Shortage of staff has been a consistent restraint, though numbers of compliance employees have recently risen steeply, by 30-100% over 2-3 years in cases of which we have knowledge. In one foreign bank, headcount tripled, and with a parallel fall in customers this resulted in the annual compliance cost per customer rising from £60-70 to over £300 (our estimate) over less than two years.[8]

Several banks, at both ends of the size spectrum, acknowledged that there was an element of 'catch-up' in their AML/CFT processes, contributing to the step change in

[7] see www.gov.uk 'Report a Loan Shark'

[8] This was one of the few banks that gave us clear figures for headcount changes and numbers of customers so we cannot be sure how much this reflects the broader picture, though the increases in headcounts we were told of, multiplied by the increase in per-capita staff costs, adjusted, in some (especially smaller) banks, for fewer customers, suggests a 2-3 fold increase would be a reasonable estimate.

numbers of compliance staff, and in one case a recognition that temporary staff were effectively carrying out remediation. This 'catch-up' component has added to the upward pressure on compliance staff salaries and consultant fees.

One large UK bank has provided detailed back office costs in relation to on-boarding, client and transaction reviews and escalation. The majority of those retail customers (individuals and small businesses) who don't merit an escalation cost the back office £1-2 for individuals and £6-7 for small businesses in compliance costs to on-board. This would materially understate the total on-boarding costs, as many/most of such costs would be met by the frontline. However, enhanced due diligence costs are mostly met by the back office: if an alert is triggered the per-customer cost rises to £10-40, and if escalated for senior expert oversight to over £100. Further details, including for larger corporate customers, are described in Section 6.1 below.

Separately, we have also been given a range of costs of £7-20k for an external intelligence report from a compliance/investigation consultant. This would materially impact the profitability of most accounts.

Top-down estimates of regulatory costs suggest these have risen steeply in recent years. For example, figures relating to global banks in the public domain suggest huge rises in headcount and spend on compliance globally. Although these banks may be seen to be responding to extreme situations, including significant fines for AML/CFT shortcomings, the order of magnitude of cost and headcount changes is not unusual among our interviewees. Indeed one of the large UK banks (with data described in Section 4) also provided some indicative cost figures for one team managing financial crime risk including higher risk customers. In 2012, this team had a budget of c. £100k, which has now grown to over £5m.

In the UK, the BBA estimates that its members are spending at least £5bn annually collectively on core financial crime compliance including enhanced systems and controls and recruitment of staff (not including the direct costs from fines for AML/CFT breaches).

Most banks had difficulty in providing estimates for on-boarding and monitoring costs relating solely to AML/CFT. This is in part understandable since it may be difficult to distinguish between these and the parts of these processes which are necessary from an ordinary banking perspective (basic record-keeping, knowledge for future marketing, etc.). Further, compliance costs are split across various teams, e.g. front-line, administration/record-keeping and financial crime. In terms of the change in costs, the banks did not indicate that the commercial non-compliance components have changed materially, so we are comfortable ascribing the majority of cost increases to compliance-related issues.

We found little appetite within banks to share increased compliance costs for bank accounts with customers on the basis of their ML/TF risk rating, either collectively or (especially) individually. Importantly this was even if such costs could be calculated and the customer might have been willing to pay more to keep their accounts. We would identify this as a form of market failure, where a more efficient allocation of costs and resources against actual, rather than perceived, ML/TF risk could result in less derisking (with the caveat that criminals would no doubt be willing to pay for access to banking, provided that they were confident of non-detection or long delayed detection). However, there are some situations where banks believe that the underlying ML/TF risks are too great and not susceptible to mitigation by their clients. In these

cases, no amount of extra spend by the bank, however funded, would offset either the risk of criminal activity or the banks perceived regulatory responsibility for preventing it.

2.4 Mitigation of Derisking Programmes (see Section 7)

Generally, banks have told us that they are seeking much more specific guidance on managing high-risk relationships of the types that have led to account exit or refusal, if there is a criticism from regulators and government that they are behaving improperly. The revised Joint Money Laundering Steering Group (JMLSG) guidance relating to MSBs is regarded as helpful by some, whilst others believe it adds nothing to their current practices and it certainly falls well short of a safe harbour, despite some (predominantly US) literature suggesting that it provides one.

Mitigation attempts using public statements such as those made by FATF, FCA and US regulators are regarded by banks as somewhat missing the mark, focusing as they do on 'wholesale v case-by-case' derisking, rather than addressing the underlying issues.

Recent fines for egregious AML/CFT breaches have clearly led to a more risk-averse attitude to ML and (particularly) TF risks. Attempts have been made by regulators to mitigate bankers' fears by pointing out that fines have not been levied for banking MSBs or for failure in controls in a bank's customer, but rather for serious failures in controls in the banks themselves.

However, there is no evidence that this reassurance has had any particular effect (including no effect) on derisking behaviour. Indeed, given bankers' perception that the global jurisdiction claimed by the US regulators and courts can place their conduct anywhere under sanction, it is not clear what reliance should rationally be placed on such reassurances from their local supervisors by non-US institutions who rely on access to the US markets: although US Federal authorities have joined in the reassurance, and might be expected to apply this to their own decisions on penalties, concerns were still expressed about the possibilities of future actions against firms and individuals by US supervisors.

2.5 Concluding Remarks

In conclusion, we have found that banks take the derisking issue seriously and are mindful of their obligations to treat customers fairly and of the financial inclusion agenda. They believe they are attempting to apply the RBA to financial crime in an even-handed and objective fashion, given inherent uncertainties about how customers will behave and how supervisors/courts will construe and react to their own blameworthiness in relation to misconduct in the accounts they hold.

It is clear to us that over recent years banks have developed (and are still developing) policies and procedures in this area, to set risk appetites, identify and manage high-risk relationships and to attempt to deal equitably with those found to be outside appetite. In some circumstances banks are prepared to enter into dialogue with customers when they are thinking of exiting the relationship (and in some cases to have a formal appeals process once such a decision has been communicated); to attempt to assist them remediate issues (such as poor financial crime controls); and to facilitate access to banking at another institution (for example, by extending notice periods).

Inevitably, there will always be occasions when banks will wish to exit a relationship without consultation and as rapidly as possible, particularly where there are crystallised financial crime issues involved. In such instances they will also not be comfortable with explaining the underlying reasons to customers, not least for legal reasons.

However what is also clear is that bankers' perception of their fair treatment is not shared by many victims of derisking. Each individual case can result in great distress, disruption and cost. In some cases it will also result in the closure of long-standing, historically problem-free and (from their owners' perspective at least) low risk businesses. These feelings are exacerbated when a long-standing relationship with a bank is terminated not with the forms of dialogue and appeal mentioned above, but rather with 'no discussion'.

We have found enormous frustration at the actions of banks, even amongst those customers fully supportive of the risk-based approach to financial crime, particularly at the lack of, or contradictory, communications from their bank other than a form letter mentioning unspecified risk appetite and at the banks' unwillingness to identify what, if any, remediation could reverse the decision to derisk. This may contrast with previously good relations with relationship managers or indeed with no contact from the bank at all over a long period prior to termination.

A summary of the paradox may come from one of the large UK banks, which, during a period of staff turnover and subsequent expansion, simply felt it did not have the compliance resources to monitor its entire client base. In order to fulfil its regulatory requirements it had to make tough decisions about clients it could retain without over-stretching its resources. Essentially, there was a major reduction in its risk appetite across the board. To a 'victim' of this process, who may have been with a bank for many years, such a decision would seem inherently unreasonable and unfair.

There appears to be no 'silver bullet' for the derisking issue. Potential solutions may lie in balancing of costs and risks between banks and high risk sectors (which may partly occur through market mechanisms) and a better developed understanding of how to measure ML/TF risk on a 'case by case' basis. Current risk assessment tools may identify as high risk the 'good' customers within a particular sector, as well as the 'bad' (those intent on abusing the financial system for criminal purposes) and the 'negligent' (those who take insufficient care to safeguard the financial system from abuse by their own customers). In the absence of an understanding, shared by supervisors and banks, of how risk can reasonably be judged at a detailed level, and the acceptance of this understanding as legitimate by businesses and other customers, dissatisfaction over derisking will continue.

3 DRIVERS OF DERISKING

The FCA asked that the Study look at the following questions:

- *Research into the reasons underpinning banks' decisions to close accounts or restrict access for new customers including an assessment of, where there are multiple drivers, which considerations, if any, are pre-eminent.*

- *An estimate of the numbers of customers that have been affected in some way by the banks' derisking programmes.*

- *Which types of customers have been affected by banks' derisking programmes? In addition any insight in to the possible future direction of derisking by banks.*

3.1 Context

Consideration of the drivers of derisking has to be placed in a wider context of developments in the banking and regulatory world. Various factors need to be taken in to account when considering the current approach to risk generally by banks.

Stricter prudential requirements imposed by regulators have led to higher cost of, and a need for more, regulatory capital and a general environment where banks seek to reduce risk weighted assets, cut costs and their overall risk profile.

Post-global financial crisis realignment and entrenchment of business has manifested itself in banks offloading parts of their operations, and in particular a move to pull out of non-core business and jurisdictions. In the derisking context this has an impact both in account closures for those in the non-core areas and for those seeking to open accounts, who find their choice of institutions restricted.

Banks and bankers are more risk averse, both generally and particularly in relation to personal and institutional accountability for their actions anywhere in the world. The impact of DPAs and other legal and regulatory actions has increasingly included very significant fines (particularly in the AML/CFT field), the impacts of which go well beyond the direct costs of fines and remediation programmes. In addition to the substantial fines, some agreed settlements of regulatory action have also included what might be called regulatory derisking – restrictions on business imposed as part of regulatory settlement for the firm involved. Examples have included loss of US dollar clearing and, in an FCA case, a temporary restriction (for a period of 126 days), in respect of its regulated activities only, on acquiring new customers that were resident or incorporated in "high risk' jurisdictions"[9]. These actions contribute, presumably as intended, to banks generally paying much closer attention to their own compliance, and particularly ML/TF, risks.

The risk-based approach (RBA) to AML/CFT is not new; indeed it has been a key principle of AML/CFT for nearly a decade. The EU 3rd Money Laundering Directive, implemented in the UK through the Money Laundering Regulations 2007, required banks to implement RBA policies and procedures. Banks accept the need for an RBA,

[9] In this case defined as a jurisdiction scoring 60 or less on the Transparency International Corruption Perceptions Index. http://www.fca.org.uk/your-fca/documents/final-notices/2015/bank-of-beirut-uk-ltd

and see an effective implementation of RBA approaches as one-way of keeping their compliance costs under control.

However, we found a clear feeling that at the practical level of risk assessment and mitigations the RBA is not yet fully evolved, certainly compared to the measurement of other types of risk, such as operational or credit. One of our interviewees contrasted 300 years of experience in banks measuring those sorts of losses, compared to a much shorter timescale for ML/TF risks, which in any case typically do not incur losses for the banks. The statistical basis for ML/TF risk measurement is not robust.

In addition the banks see a greater regulatory focus on risk management, which they expect the further emphasis on risk in the revised FATF standards and the forthcoming 4MLD will exacerbate.

The BBA said in their response to the Department of Business, Innovation & Skills (BIS) Cutting Red Tape Review in to the Effectiveness of the UK's AML Regime[10] (our emphasis):

> '*A cost-benefit analysis of the regime, alongside work to develop a* ***common understanding of the highest priority risks****, can provide the basis for a strategy that sets out how our collective resources can be most effectively deployed to respond to financial crime.*'
>
> ...
>
> *'However, whilst the FCA and the banking industry are in agreement at a strategic policy level that a risk based approach to financial crime is most effective, there can be* ***differences of view on the practical application****.*'

In particular, banks believe that better information sharing between the public and private sectors would enhance their ability to identify risks beyond the somewhat generalised models described below. It seems inevitable that a proportion, possibly a significant proportion, of customers currently identified as belonging to a high risk cohort, in fact pose a lesser risk.

As we discuss below, in the absence of distinguishing information on a) those at risk of exploitation by criminals or b) intent on exploiting the banks themselves, 'good' customers with profiles similar to these two groups will find themselves grouped together with them by risk assessment tools. It is almost inevitable, given large populations of accounts and imprecise measures of financial crime risk, that significant numbers of those classified high risk (and indeed derisked) would not have posed any significant financial crime risk when measured by incidence of events. Put simply, the appearance of (for example) MSBs in a large number of law enforcement investigations does not necessarily imply that a large number of MSBs are significantly abused for financial crime purposes.

Legal risk relating to civil court actions is an increasing concern, driven in particular by US cases relating to foreign banks allegedly facilitating terrorist finance (TF). This is notwithstanding the recent successful appeal by Arab Bank in a case brought by non-US victims of terrorism. Banks accept there is also legal risk in closing bank accounts,

[10] BBA response to Cutting Red Tape Review - Effectiveness of the UK's AML Regime: https://www.bba.org.uk/policy/bba-consultation-responses/bba-response-to-cutting-red-tape-review-effectiveness-of-the-uks-aml-regime/

and there have been a small number of cases of action taken against banks, but the unquantifiable possible impact of a TF case – civil, criminal or regulatory - outweighs this by a large margin in banks' estimation.

3.2 Derisking – Policy or Consequence of RBA?

A common theme in the literature, including regulatory statements, on derisking is a distinction between 'wholesale' and 'case-by-case' derisking. For example, in October 2015, the FATF said[11]:

> *'What is not in line with the FATF standards is the wholesale cutting loose of entire classes of customer, without taking into account, seriously and comprehensively, their level of risk or risk mitigation measures for individual customers within a particular sector.'*

The FCA itself stated in April 2015[12]:

> *'But the risk-based approach does not require banks to deal generically with whole categories of customers or potential customers: instead, we expect banks to recognise that the risk associated with different individual business relationships within a single broad category varies, and to manage that risk appropriately.'*

3.2.1 Assessing customer risks

Banks expressed a certain degree of frustration with such statements. There is a possibility that they describe, to some extent, a distinction without a difference in that a bank's decision on risk assessment may be the same whether it is undertaken on a case by case basis or wholesale basis, because the factors applied will not vary too much.

The risk-based approach to financial crime is generally built around a framework of assessing customers by identifying the risk posed by various factors relating to that customer relationship, such as:

- Sector, occupation, types of business
- Geography and jurisdiction risk
- Political risk
- Distribution/delivery channels
- Product or services that customer requires or uses

There is, as yet, no broadly agreed quantitative method for assessing these risk factors, individually or collectively. Banks are expected to develop their own measures and weightings, although some commentators suggest that there is not, and may never be, sufficient data to do more than a broad subjective assessment[13]. Professor Peter Reuter

[11] *FATF takes action to tackle de-risking*, 23 October 2015: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-action-to-tackle-de-risking.html

[12] *Derisking: Banks' management of money-laundering risk - FCA expectations,* 27 April 2015: https://www.fca.org.uk/about/what/enforcing/money-laundering/derisking

[13] See, for example, *Global Surveillance of Dirty Money: Assessing Assessments of Regimes to Control Money-Laundering and Combat the Financing of Terrorism*, 2014, Halliday, Levi, Reuter, Center on Law and Globalization.

has said, "*the science of risk analysis is poorly developed for money laundering, and it is currently impossible to judge relative risk on an objective and systematic basis.*"[14]

Therefore, applying these risk factors to a particular relationship may, in effect, *require* a generic approach, such as using lists of high risk sectors or countries, which we have found in the AML/CFT RBA policies of several large UK banks. We expect similar risk attributes to be used by most banks, as this approach is enshrined in the FCA Financial Crime Guide and JMLSG Guidance. Larger institutions have the resources to carry out their own research, whilst smaller ones may rely more on commercially, or freely, available data and lists from external suppliers, but any such assessment ultimately relies on a finite number of sources, and many criteria are essentially about the nature of the customer's business. Box 1 outlines some current UK guidance to financial institutions on these issues.

[14] *Report Questions Global Fight against Money Laundering and Terrorism*, American Bar Foundation Press Release, 30 January 2014: http://www.americanbarfoundation.org/news/475

Box 1: UK Guidance on Customer Risk Assessment

JMLSG Guidance, Part I

4.15: Identification of the money laundering or terrorist financing risks, to the extent that such terrorist financing risk can be identified, of ***customers or categories of customers****, and transactions will allow firms to determine and implement proportionate measures and controls to mitigate these risks.*

4.26: ***Countries may be assessed using publicly available indices*** *from HM Treasury Sanctions, FATF high-risk and non-cooperative jurisdictions, MONEYVAL evaluations, Transparency International Corruption Perception Index, FCO Human Rights Report, UK Trade and Investment overseas country risk pages and quality of regulation.*

4.29 Money laundering and terrorist financing risks may be measured using a number of factors. Application of risk categories to customers/situations can then provide a strategy for managing potential risks by enabling firms to subject customers to proportionate controls and oversight. ***The key risk criteria are: country or geographic risk; customer risk; and product/services risk.*** *The weight given to these criteria (individually or in combination) in assessing the overall risk of potential money laundering may vary from one institution to another, depending on their respective circumstances. Consequently, firms have to make their own determination as to the risk weights. Parameters set by law or regulation may limit a firm's discretion.*

FCA Financial Crime Guide

Box 3.3 Risk assessment, Examples of good practice…

Consideration of money-laundering risk associated with individual business relationships takes account of factors such as:

- *company structures;*
- *political connections;*
- *country risk;*
- *the customer's or beneficial owner's reputation;*
- *source of wealth;*
- *source of funds;*
- *expected account activity;*
- *sector risk; and*
- *involvement in public contracts.*

Box 3.6 Handling higher-risk situations

Situations that present a higher money-laundering risk might include, but are not restricted to: ***customers linked to higher-risk countries or business sectors****; or who have unnecessarily complex or opaque beneficial ownership structures; and transactions which are unusual, lack an obvious economic or lawful purpose, are complex or large or might lend themselves to anonymity.*

What may differ between banks is risk appetite, i.e. the amount of ML/TF and other financial crime residual risk that a particular institution is prepared to take on, and their view of the efficacy of their own management of those risks, which results in the assessment of residual risk. Although it is a matter for banks (subject to regulatory judgments) how to manage their risks, the international standard and regulatory guidance/expectations focus on two types of mitigation:

- Enhanced Due Diligence
- Ongoing Monitoring

Of course, some risk factors that lead to a higher rating may not be amenable to such mitigation. For example, if the concern is around the ability of third parties to make payments through an account, with little or no visibility to a bank, it may conclude that they cannot effectively mitigate that risk, however much they spend on monitoring the account (because the detail that they believe they require is not available). Similarly, risk relating to external factors cannot be reduced using such tools – for example, geographic risk, perhaps relating to lack of regulation or a terrorist finance threat, as in the Somalia example, is beyond the scope of banks' risk mitigations, although firms with a presence in a region or jurisdiction may be able to draw more comfort from their superior knowledge of the situation.

However, it is clear that banks regard adjustments in the nature of the customer relationships they maintain as an extremely important part of their risk mitigation toolbox. Typically, beyond Enhanced Due Diligence (EDD) and ongoing monitoring such interventions may include:

- Exit some, but not all, business areas from that relationship
- Restricting the products supplied or offered to that customer
- Exiting the relationship entirely

Banks are adamant that they do not 'wholesale derisk'. To the extent it is possible, we tested this by discussing, and reviewing copies of high level risk appetite and policy statements, as we consider that 'wholesale' can be characterised as a conscious decision not to do business with particular sectors.

3.2.2 Risk appetites

We found no overt policies of not banking entire sectors for AML/CFT reasons. Some of our interlocutors feel this may have been less circumspect in previous years, when they believe some banks did have such policies, stated or unstated, but that banks are now approaching the issue in a more considered way. However, it is true that some banks may not bank particular types of businesses for commercial or 'bank culture' reasons.

This may be because the bank has no background in particular regions, or no interest or capacity to supply certain industry sectors or products. One of the larger banks stated that it would be irresponsible to serve clients in sectors or geographies where the bank did not have competence to understand the potential risks. There may also be top-level strategic issues, one example being an ethical or reputational risk stance relating to providing banking services to defence-related companies. These positions restrict the available market to those seeking banking services, of course – not all banks will bank all types of customer.

However, we find that ML/TF risk appetite is difficult to articulate and measure, perhaps unsurprisingly. Banks are still developing this art and in particular find it difficult to "price" (in broad terms) ML/TF risk, as well as a reluctance to adopt an explicit compliance cost-base for pricing accounts, as described later in Section 6. Some banks have specific risk appetite statements relating to certain sectors, such as MSBs and virtual currency exchanges. However, generally these statements do not amount to a blanket ban on such businesses, although they may include strong acceptance requirements relating to the nature of the customer and their operations. From our knowledge of the experiences of some of those affected by derisking (see Section 5 below), it is possible that these requirements get translated, explicitly or strongly implicitly, to an effective total ban at a local business level when dealing with some customers. The data are not sufficient to say whether this is improving over time, as policies get imbedded in operational practices.

In some cases, on-boarding may be an exception process or may include a revenue requirement, as well as enhanced customer due diligence checks. It is also important to note that on-boarding and exit decisions frequently lie with the first line, which will have discretion to apply stronger controls (which may include exit or refusal), but not weaker controls than those mandated by the second line. Box 2 below outlines some statements about risk appetite.

Box 2: Examples of Risk Appetite Statements

Bank I focuses on clients where there is sufficient mutually attractive current or future business, aligned to our risk appetite and the Bank's core values, to justify the investment required to satisfy all internal and external Regulatory due diligence requirements.

Bank II is committed in its efforts to counter financial crime and to comply with applicable UK law and sanctions regulations. Bank will apply strong controls to manage these risks and it has a minimal tolerance for residual Financial Crime risk

Bank III is committed to complying with its legal and regulatory responsibilities in relation to Anti-Money Laundering and Counter Terrorist Financing and has no appetite for non-compliance. Anti-Money Laundering legislation allows the Bank to adopt a risk based approach to the way in which it complies with these obligations. This enables the Bank to focus its control framework on those customers, products, channels and jurisdictions that carry a greater ML/TF risk.

Bank IV has no appetite to open or maintain a direct active relationship with an Individual or Entity for whom:

- The required level of due diligence has not been or cannot be completed; or
- The business is unable to provide the level of ongoing scrutiny necessary to ensure that any suspicions of money laundering are promptly identified and reported; or
- There is proven or credible evidence of involvement in financial crime.

Examples of statements about specific sectors:

Bank will not provide USD Clearing to third party banks

Bank shall not provide services to embedded correspondents

Bank has a specific risk appetite for MSBs which is reviewed and approved by the Group Financial Crime Committee. The MSB risk appetite statement does not prohibit business with MSBs, but instead requires that Bank maintains and takes on MSB business in accordance with the requirements in Policy

Two reasons suggested for increased bank risk aversion were the increasing focus on the business line 'owning' the risk posed by a customer, and the focus on personal liability. The latter was both through the Senior Management regime and a perceived regulatory narrative that individuals will more likely be held liable in the future than in the past. The question as to whether this is for reputational or cost/complexity reasons remains open.

For example, it was suggested to us that even where the second line felt a particular risk could be managed, the first line would view the 'hassle' of doing so and its associated cost as not worth the potential reputational damage (by its nature, a risk-based approach accepts the possibility of failure). This could be true even when the likelihood of a large fine for AML/CFT failings appears to be quite remote, although banks do not make that calculation explicitly. A clear decision to derisk taken at an early stage is also easier to manage internally and externally, compared to taking on a potentially difficult relationship, which will need regular review and decision making, and may result in a decision to exit, which itself carries costs (and a subsequent likelihood of complaints).

3.2.3 Policies leading to derisking

Risk appetite and approach have to be operationalised, through implementing policies and procedures. Typically this will involve a combination of risk assessing a particular customer or relationship; setting identification and verification requirements (both generically and in particular cases – for example, for certain types of customer and sector); and establishing monitoring regimes. The extent of monitoring, and requirements to review the relationship (for example to re-verify identity) will be informed by the risk rating applied to the customer. One fairly standard example would be to review high-risk annually, medium-risk every three years and low-risk every five years. We have heard of more frequent review periods, particularly for high-risk customers such PEPs, where the highest-risk may be reviewed every three months.

Inevitably, perhaps, risk assessment tools will score similar customers in a similar way, particularly at the large retail end of the market, either for individuals or SMEs. For reasons of scale there has to be a generic approach taken to characterisation. Thus it is entirely feasible that a set of similar customers may fall outside risk appetite (as expressed through the risk scoring produced by the model) and as a result be exited.

Banks stress that generally they lack access to privileged information, such as criminal intelligence, which they say could help them make a more granular distinction between similar customers. It is of course a moot point, and there are other issues such as whether such information should be made available and, if so, to whom and on what conditions (including financial conditions).

Where the bank has a current relationship with a customer, it can factor more information into the risk assessment, drawing on the manner of the running of the account(s) previously and accumulation of other data, including identification and ownership, over the course of the relationship. When considering a new relationship, this detail is generally not available, given the absence of inter-bank information sharing of confidential data.

This is why we say there may be a 'distinction without a difference'. Through applying their risk assessment tools to a certain customer base, banks may define a set of customers outside their risk appetite. By the nature of the model, those customers (or sub-sets of them) are likely to share certain characteristics of geography, sector,

business type etc. From the banks point of view that is simply a result of applying the risk-based approach in the manner laid out in international standards and regulatory guidance/statements – i.e. on a case-by-case basis, taking into account all the attributes of the customer and relationship.

From the affected customers' point of view, this can look like 'wholesale' derisking. A critical view could also be that it is always possible to 'set the dials' of a risk model to achieve a pre-determined desired result, but our interviewees insisted that they are doing their best to apply the risk-based approach as required/expected and, so long as obedience to managing AML/CFT risks is prioritised, their logic is not flawed.

3.2.4 Decisions to derisk

Banks say they take decisions to restrict or exit relationships very seriously. Various mechanisms were described, usually involving a review by some form of committee, to ensure fairness and consistency. The decisions need to be taken to a set of consistent standards (although it can be difficult to compare risk ratings across different types of business, particularly in large banks) and making an exception on an individual relationship basis would undermine this, and in the banks' view – rightly or wrongly - be regarded dimly by regulators. Indeed, such consistency would produce the uniformity of derisking without derisking being an active goal: it is an unintended consequence of common judgement using shared criteria.

Banks have processes in place to consider keeping or exiting customer relationships on a case-by-case basis. Once a customer has been identified as being outside a bank's risk appetite, any decision to retain must be based on solid information showing that, although falling within the 'too high' risk cohort, this *particular* customer in fact poses a lower risk. In a sense it is an attempt to prove a negative and it is difficult to establish clear criteria for how this might be done.

This can be seen most starkly when dealing with a class of customers that banks are obliged to treat as high risk, namely Politically Exposed Person (PEPs) outside of the UK. In fact, of course, most PEPs are not criminals, or cannot be shown to be so on the basis of publicly available information, and banks have evolved more complex risk assessment scoring to cater for this situation. For example they assign 'high-low, high-medium and high-high' risk scores to different categories of PEPs in order to apply a risk-based approach (RBA) to take-on, on-going monitoring and retention activity, notwithstanding the legal obligation to carry out EDD on PEPs.

Issues such as these have led the BBA to call for discussions to promote a closer common understanding with the FCA on the practical application of the RBA.[15] Perhaps, similar approaches could be applied to other (commonly accepted) ML/TF high or higher risk sectors – for example, if certain types of MSBs operating in certain markets are regarded as high risk, what characteristics, if any, might identify the 'good' from the 'bad' or 'negligent' within that category?

Once a decision has been reached that the risk of a particular customer or set of customers is too high for the relationship to continue, the banks' expectation is that regulators would want them to exit that relationship as quickly as possible (within the

[15] BBA response to the Cutting Red Tape Review – Effectiveness of the UK's AML Regime, November 2015: https://www.bba.org.uk/policy/bba-consultation-responses/bba-response-to-cutting-red-tape-review-effectiveness-of-the-uks-aml-regime/

law and their contractual terms and conditions, and without tipping off) in order to mitigate and minimise the financial crime risk, even where there is no history of incidences.

Recognising that 're-banking' can take considerably longer than the notice period in terms and conditions, banks have on some occasions extended the amount of time in order to facilitate the customer finding alternative arrangements, if they can make them. There are also examples of banks working with some customers to address the identified risks, for example where they relate to the level of AML/CFT controls operated by the customer. Of course, the more crystallised the risk or, inevitably, the less the potential return, the less likely banks seem to make such accommodations. In Section 6 we report how rare the derisked claim such accommodations are.

All decisions to exit, or restrict, a relationship come from some form of review, either at take-on or during the course of the relationship. Triggers might include:

- Regular review of risk-rated clients – so high risk will be done more frequently as required (or perceived to be required) by regulators (or monitors acting *qua* regulators) and in accordance with the bank's processes.
- As required by regulatory agreements/settlements – for example, a look back at a particular line of business.
- Account or relationship activity, reaction to external guidance, news etc or other trigger events, examples of which are shown in Box 3.

Box 3: Examples of Trigger Events Provided by Banks

- Identification of a PEP;
- Change of ownership, structure, material change in turnover;
- Change in core business strategy
- Early surrender of a product;
- Change of name, address or addition of another party to an account;
- Reactivation of a dormant account;
- Identification of adverse media;
- Identification of a designated individual or entity;
- Receipt of a Court Production Order;
- Multiple disclosures to a Financial Intelligence Unit (FIU).

As can be seen, such reviews are often part of the financial crime risk management framework. However, it does not follow that decisions to exit, or restrict, relationships arising from such a review will be exclusively or indeed predominantly made for financial crime risk management reasons. Justifications leading to account closure or restriction may also include:

- Failed background checks, including failure to supply adequate and verifiable identification
- Fraud markers (e.g. adverse Cifas checks)
- General credit/operational risk reasons
- Dormant or non-profitable accounts

- Accounts not being used for declared purposes, particularly in sectors outside the bank's core business

Occasionally, however, review activity will lead to financial crime concerns. This is a relatively rare occurrence compared to the numbers of relationships reviewed. These concerns may be characterised as taking one of three broad forms:

- Management of financial crime *issues*: e.g. actual fraud detected or known money laundering investigations. Banks manage these cases in close cooperation with the relevant investigating agency (which can be an overseas one), but will need to come to an independent decision on continuing or exiting the accounts, on the basis of the risk posed.
- Management of financial crime *suspicions*: where an internal or external suspicion report has been made. These cases are managed primarily by the bank in isolation, given the very low ratio of investigations to Suspicious Activity Reports (SARs) made. They may lead to decisions to exit relationships, either on strict criteria (such as '3 strikes and out') and/or more nuanced assessment case-by-case review (such as media reports of links to an organised crime figure or a notorious well-known PEP).
- Management of financial crime *risk* – which is where most of what is called derisking probably lies, particularly where groups of similar customers are affected. The combination of risk factors relating to the customer is so high that the bank cannot satisfy itself that it can be mitigated by the combination of controls operated by the bank and by the customer itself (where appropriate, for example, when the customer itself is part of the AML/CFT regulated sector). Note that such decisions typically are made without regard to the collateral damage caused to the client or the client's customers/beneficiaries, although banks are well aware of such impacts.

3.3 Types of Customers Affected

As with recent surveys, we sensed some push-back from banks when asked to describe the types of customers likely to fall outside their risk appetite. As they do not accept they are derisking in any wholesale way, they naturally portray this in risk assessment terms and sector risk is only one component of their ML/TF risk modelling.

One interesting line of study may be exactly *how* risk factors are combined to result in a high (or indeed higher or highest) risk score that may leave a customer in peril of account closure. In one example, a single factor high rating (country risk being specifically mentioned) alone could be treated via exception procedures so as not to drive the customer into a high risk category, subject to other factor ratings. Another bank told us of the difficulty of a change in country risk rating, for example based on external lists, having a significant effect on a large proportion of their customer base, so only being applied to new, not existing, relationships.

There is a degree of commonality to the attributes regarded as identifying high risk sectors and types of business. This is perhaps unsurprising, as banks rely (and are expected to rely) on sources such as FATF standards and guidance, JMLSG guidance and typologies emerging from law enforcement. In all the ML/TF high risk sectors identified, there is some form of signalling from the authorities that the sector does pose some form of threat or have inherent vulnerabilities.

This may range from a legal requirement to regard some customers as high risk (e.g. non-domestic PEPs) or a cumulative impression gained from various statements (e.g. the gambling sector, where casinos are singled out for specific measures under the FATF standards above and beyond other designated non-financial businesses and professions).

Common sectors identified in bank risk assessment methodologies as posing high risk include:

- PEPs
- Correspondent Banking
- MSBs
- Charities
- Casinos and Internet Gambling
- Defence/Arms

An example of signalling of these sectors can be found in Part II of the JMLSG Guidance, which lists examples of higher risk situations for retail banks, as shown in Box 4.

Box 4: JMLSG Guidance Part II, 1.36

Examples of higher risk situations are:

- High cash turnover businesses: casinos, bars, clubs, taxi firms, launderettes, takeaway restaurants
- Money service businesses: cheque encashment agencies, bureaux de change, money transmitters
- Gaming and gambling businesses
- Computer/high technology/telecom/mobile phone sales and distribution, noting especially the high propensity of this sector to VAT 'Carousel' fraud
- Companies registered in one offshore jurisdiction as a non-resident company with no local operations but managed out of another, or where a company is registered in a high risk jurisdiction, or where beneficial owners with significant interests in the company are resident in a high risk jurisdiction
- Unregistered charities based/headquartered outside the UK, 'foundations', cultural associations particularly if centred on certain target groups, including specific ethnic communities, whether based in or outside the UK

Within these sectors, risk ratings will be affected by other attributes, again frequently based on one or more forms of guidance. For example, country risk will be assessed in relation to ownership and incorporation, but also trade and financial links. The nature of the relationship the customer has with the bank is also a risk factor, and the types of transactions it undertakes are important. As described above, this leads to firms with similar characteristics of business model and areas of operation being similarly risk-rated, and therefore at similar risk of derisking.

One interesting finding was that UK casinos have apparently not been affected by derisking, even though they carry some perception of higher risk and are found in lists of high risk customers (even though the NRA assesses the risk of the sector as 'Low'). Banks certainly have a lack of visibility on the underlying customers. The sector has been expected to supply more detailed information on their AML/CFT controls to their bankers, but we have found no concerns about maintaining their banking facilities.

Although the industry is largely cash-based and the banks have little visibility of underlying customers, those customers are generally unable to use casinos to transfer money to other individuals or jurisdictions, which may provide comfort to the banks; there may also be a perception of good quality regulation and compliance functions. There is some evidence in the public domain of independent and on-course bookmakers being affected by a consolidation in services being supplied to the gambling sector.

The defence sector is often cited, but our findings are that concerns relate more to reputation and ethical issues, than specific ML/TF concerns (see Section 5.7 for more).

With FinTech, banks cite commercial decisions relating to start-ups with little understood business models and underdeveloped regulation in the field as concerns, although they also have ML/TF vulnerability concerns around virtual currencies, for example.

We draw the following conclusions based on bank adduced evidence:

- SMEs are more likely to be derisked in many cases than larger firms in the same sector. This may arise from either a revenue requirement for customers in certain sectors (used to offset potential compliance costs, but see below for more on this) or use of size as a proxy for compliance effectiveness. Banks may derive more comfort from compliance functions that looks familiar in terms of structure and operation, in particular access to data and staff to carry out controls. There may also be an element of legal risk mitigation with an expectation that, in the event of a compliance failure, regulators might be more likely to lay blame at the door of a larger, regulated customer, than their bank.
- Country risk is an important element leading to derisking, but some of the lists used, particularly by smaller institutions, may not be providing a suitable risk factor. As examples, the Transparency International (TI) Corruption Perceptions Index and the FATF list of countries with strategic AML/CFT deficiencies, both of which we understand are used in isolation or combination, were designed for specific purposes, and may not obviously provide a good way of measuring the risk in individual specific customer relationships.
- Relationships involving cash handling and/or transfer of value (particularly cross-border) unsurprisingly feature very often in derisking. Using a bank to facilitate transfers or other activity on behalf of customers on whom the bank is broadly unsighted are regarded as posing risk to the bank– thus MSBs in general, remittances in particular; NGOs (primarily around transferring money to difficult destinations); and correspondent banking relationships are at risk, as very well documented in the literature on derisking.

Future direction of affected sectors is difficult to analyse. To an extent it should follow changes in risk perceptions. Banks have been specifically encouraging smaller, riskier firms to move under the umbrella of larger firms (for example, one bank lists only two money transmitters it will bank, any others must become part of those networks or not be banked). If these firms are subsequently found to be unable to manage the increasingly concentrated risk the banks are currently transferring, there may be further and potentially more damaging derisking.

Other specific issues mentioned to us so far include crowd-funding based activity (e.g. concerns over how to describe beneficial ownership); law firms, given particular interpretations of 4MLD, which suggest that many individual client accounts will need to be opened with associated costs; and more issues in interbank relationships, again because of a view that 4MLD will bring more activities into the definition of correspondent banking.

4 ACCOUNT CLOSURE DATA FROM BANKS

The data in this section come from interviews with, and written data disclosures from, 23 banks.

The following describes some of the data we received from banks on their account turnover, with a focus on relationship exits of non-banks for AML/CFT/sanctions or broadly financial crime-related reasons. We received input from a modest number of UK mid-sized banks, so most of the data are from larger UK banks and from UK branches and subsidiaries of foreign banks.

It is interesting that the large UK banks are, in general, not tracking account turnover (or derisking) by sector or subsector, and in order to answer our data requests, they had to manually compile estimates. Also, they found it difficult to collate the precise reasons for exits, either because of the lack of clear coding, or because they were not confident that such coding by client-facing staff would be consistent. Nonetheless, three of the large UK banks were able to give us an estimate of accounts closed for reasons somewhat related to financial crime risk. We have not compared these figures side-by-side due to differences of definition as well as perimeter.

In general, at the large UK banks, accounts are being opened, as a proportion of total accounts, at a rate of 5-15% p.a., and even faster for businesses at one of them. There is more variation in the rate of closures – thus, one bank has seen shrinking personal accounts, while another is seeing strong growth in this area. One reason for such variation is the timing of periodic dormant account culls. The absolute numbers are huge, of course, at millions of personal accounts and hundreds of thousands of business accounts p.a.

Tracking the proportionately tiny number of closures linked to financial crime concerns within this immense dataset is thus inherently challenging, especially if the reason for closure is primarily commercial, with a small component of the equation relating to 'increased compliance costs'. Even so, across two large UK banks, around 1,000 personal accounts and 600 business/corporate accounts are closed per month for being, essentially, outside risk appetite.

Our data from higher risk sectors in the large UK banks is too patchy for clear cut conclusions. The bank which provided data on high risk sector account turnover was unable to provide consistent well defined data on closures for financial crime-type reasons. Nonetheless this bank showed two flurries of MSB closures, in 2013 and 2014, for definitions that might represent financial crime-related reviews, while another bank had carried out a remediation review of its MSB portfolio in 2013, which resulted in a sharp fall in client numbers.

In the Charities sector, one bank has been opening accounts at a rate of 12-13% of total charity accounts p.a. during 2012-4. Its underlying rate of closures, mostly for reasons described as 'no longer required' and 'customer ceased trading' have run at around 5% p.a., with the exception of a review of dormant accounts in 2012-3, when over 10% of its charities accounts were found to be sufficiently dormant to be closed. We estimate its financial crime closures at around 1% of closures p.a. or less than 0.1% of extant accounts.

Finally, our data gathering across other banks produced a wide range of outcomes. To aggregate and paraphrase:

- "We have not been affected and have felt no need to change our client list or service offering" (around 10-20% of banks, though this is likely to be understated due to 'the silence of the unaffected')
- "We have taken into account heightened sensitivities, have reviewed our client lists, but made very few changes" (also 10-20%)
- "We have taken into account heightened sensitivities, and have also carried out a strategic review, resulting in a return to core business areas. Therefore we have reviewed our client lists, and cut 10-30% on a case by case basis" (30-40%)
- "We are under pressure from our correspondent banking partners…" or "we may come under pressure… and therefore have begun a process of remediation and case-by-case closures" (30-40%, though likely overstated due to 'silence of the unaffected')
- In one case "we could no longer justify an entire business line, we discussed it with our regulator before shutting it down"

We would emphasise that many of the client exits alluded to above result from a 'perfect storm' of multiple impacts, including higher capital requirements, higher costs for compliance resource, higher levels of sanctions, a perception of higher risk of sanctions, and specific US private legal cases, *inter alia*, which in many banks provided a suitable context for a strategic review. The implication is that many account closures relate in large part to changes in the perimeters of business lines and geography, rather than for purely financial crime reasons. The evidence does not enable us to conclude that without those reasons the accounts would have remained open.

4.1 Large UK Bank 1 - Account Turnover

Table 1 shows the account turnover over a four year period at a large UK bank, presented as the number of accounts opened or closed in a 12 month period as a proportion of the previous year-end total for that category.

Personal accounts grew strongly from 2010 (not shown) to 2012 and then began to shrink. PEPS, which accounted for c.0.05% of personal accounts, saw a significant shrinkage over the period. Sole trader accounts shrank while SMEs grew strongly over the period. Corporates saw the highest turnover and grew strongly. At the end of the period the ratio of sole traders to SMEs to corporates was approx. 3:10:2.

Table 1 Accounts opened and closed as a % of previous year-end total

	2011	2012	2013	2014
Personal				
Opened	15.1%	16.7%	13.1%	11.3%
Closed	10.2%	15.5%	14.2%	13.0%
o/w PEPs				
Opened	10.9%	12.7%	9.9%	8.9%
Closed	10.9%	17.6%	19.1%	15.6%
Business				
Sole Traders				
Opened	21.5%	20.3%	18.3%	11.9%
Closed	18.7%	23.8%	18.7%	15.2%
SME				
Opened	19.0%	21.9%	21.7%	18.3%
Closed	13.1%	18.9%	13.6%	13.9%
Corporate				
Opened	34.8%	20.9%	21.7%	24.5%
Closed	20.8%	18.6%	16.9%	15.6%

Table 2 shows account turnover for 'high risk' sectors on the same basis. We understand these are classified primarily as SMEs and corporates. It is worth noting that, for many categories, this bank did not have clear cut customer codes for easy identification, and on occasion had to search free text descriptions to categorise them. Therefore the sub-categories below should be assumed, in some cases, to be best guesses.

Table 2 Accounts opened and closed as a % of previous year-end total- Business Sub Category (High risk sectors)

	2011	2012	2013	2014
Charities				
Opened	7.8%	12.4%	13.5%	12.0%
Closed	5.2%	14.8%	7.4%	4.9%
Defence				
Opened	31.7%	23.3%	26.5%	15.8%
Closed	14.4%	9.8%	10.3%	10.2%
Embassies				
Opened	4.8%	37.5%	24.3%	38.9%
Closed	8.8%	16.1%	5.6%	10.7%
Gambling (online)				
Opened	5.2%	10.2%	20.0%	21.0%
Closed	28.7%	25.0%	37.3%	12.9%
Gambling (traditional)				
Opened	11.6%	15.8%	14.0%	12.8%
Closed	25.9%	15.8%	10.3%	14.5%
MSBs				
Opened	21.6%	23.7%	37.2%	51.0%
Closed	12.7%	15.3%	16.3%	14.7%

For most high risk sectors, the bank has opened more accounts than it closed. This is especially true for embassies and MSBs. Gambling is the exception, especially online. In terms of absolute numbers, and assuming the majority of MSBs are SMEs, MSBs accounted for close to 1.8% of SMEs, though it is worth noting the above caveat about sector allocation.

The bank has, in addition to data for high risk sectors, provided the same data for all corporate, SME and sole trader industry sectors, but we have not included them here for reasons of space.

The same bank has also provided a breakdown of the reasons for account closures. The bank noted caveats in relation to these data, i.e. that they are dependent on the consistency of user entry, with some of the reason categories being generic. Taking charities, for example: In 2014 c.2,500 accounts were closed, o/w 59 were closed for reasons that *might* relate to compliance concerns, falling under the following descriptions

- Reason 1 "an area (branch, call centre, relationship team, etc) has some kind of concern about the customer or account", or
- Reason 2 "there have been financial crime concerns and so exit will be at the request of either the first or second 'line of defence' teams responsible".

By contrast, 1,144 closed accounts were “no longer required”, 441 were closed when the customer “ceased trading voluntarily” and 651 when the customer "ceased trading involuntarily”, and these three categories summed to 89% of closed accounts.

For comparison, 6,368 charity accounts were opened during 2014.

Looking at MSBs, 2013 closures were due primarily to "no longer required" and "customer ceased trading voluntarily" (84% combined), though 5% were recorded as being for reason 2) mentioned above. In the following year, 2014, Reason 2 was barely recorded (0.2%) while Reason 1 was very significant, accounting for 17% of exits (up from 3% in 2014). However, across the entire client base, personal and corporate, Reason 1 above was recorded for almost one third of all closures in 2014, so it is difficult to map anything more than a tiny proportion of these closures to financial crime issues. Reason 2 was noted c.2% of the time in 2013/14, so it may be reasonable to assume 2013 saw a focused review of MSBs.

4.2 Large UK Bank 2 – Account Turnover

This bank has been opening personal accounts at an annual rate of c.8% (of previous year-end total) in 2015, and closing them at a rate of less than 1%. 96% of those exited were closed for non-financial crime reasons (“at the customer’s request”), meaning around 600 per month were closed for being “outside financial crime risk appetite”. This includes accounts that have been identified as fraudulent or being associated with fraud.

Very small businesses (below £1m turnover) saw around five closures per month for financial crime (i.e. again outside financial crime risk appetite) reasons and wealth management around four closures.

Separately, this bank disclosed that just 0.02% of its retail banking relationships were with PEPs (this figure includes domestic and overseas PEPs).

In corporate banking (SMEs above £1m and larger companies), accounts are being opened at an annual rate of c.8% of the previous year-end total. Exits for being outside financial crime risk appetite are occurring at c.40 per month. 0.6% of corporate customers have some PEP component (owners, directors etc.).

This bank provided granularity on its MSB portfolio, which was reviewed in 2013. 10% of MSBs were exited at the bank’s request, while 31% were closed at the client’s request. 27% were de-classified as MSBs (and classified in other sectors). The remainder, a relatively small portfolio, were retained, after being assessed as within risk appetite, in some cases after refreshing the customer due diligence.

We do not have data from this bank, or any other, on the proportion of attempted openings which are turned down for financial crime reasons. One reason given is that many applications may not be pursued for reasons the bank may not be told.

4.3 Large UK Bank 3 – Account Turnover

This large UK bank’s management information system was not aligned with our data requests. However, its AML team provided indicative management information in answer to some queries. Volumes for accounts opened were given as ranges, typically +

or – 10-15%. We took central figures for the calculations below. Please therefore bear in mind that the data below are very much estimates.

In Table 3, we show total accounts opened in 2015 (year to November annualised) as a percentage of the total for each client segment. It also shows accounts closed for AML-related reasons, on a broad definition as described in the table note.

Table 3 Total accounts opened, and those closed for AML-linked reasons, as a % of total

	Opened	Closed*
Personal	4.5%	0.025%
Small Businesses	10%	0.013%
Corporates	14%	0.028%
Wealth	2.0%	0.045%

NB All data based on annualised 2015. **Corporates are mid-sized businesses excluding large corporates, i.e. up to £25m turnover**. * Exits based on AML or Financial Crime concerns, including some linked to commercial risk appetite decisions e.g. customers who are rated as higher risk or have clear links to sanctioned countries but are not sanctions-designated targets. A case by case review of such customers seeks to determine both the nature of the banking relationship and assess the financial crime risk. Outcome may include a decision to exit based on commercial grounds due to higher risk rating i.e. low volume account activity / bank does not act as customer's main bank.

The table shows, for example, that c.5% of the stock of small businesses are classified as Higher Risk, and that 8% of the new-to-bank small business accounts in 2015 were classified as Higher Risk.

Table 4 provides information on 'Higher Risk' accounts. These are customers/clients in each segment judged to be higher risk, with an initial rating allocated during on-boarding, and then updated on an on-going basis as a result of changes to customer circumstances or business activity. Risk rating methodology and scoring is based on, *inter alia*, nationality, country of residence or business, product type and business type.

The table shows, for example, that c.5% of the stock of small businesses are classified as Higher Risk, and that 8% of the new-to-bank small business accounts in 2015 were classified as Higher Risk.

Table 4 'Higher Risk' (HR) accounts as a % of total for each client segment, HR accounts opened (2015 annualised) as a % of HR total, HR accounts opened as % of total opened

		HR Opened	
	HR as % of total	as % of HR	as % of total opened
Personal	0.1%	1%	0.02%
Small Business	5%	17%	8%
Corporates	3%	11%	2%
Wealth	0.5%	4%	0.8%

4.4 Global Bank

Another global bank has disclosed 34 corporate and investment banking client exits (including banks) for "risk management" reasons over an approximate two year period from October 2013. There were 17 exits over this period linked to SARS, but this figure overlaps at least in part with the 34. By contrast, the number of closures in relation to strategic realignments (though we cannot exclude compliance cost being a factor) were at around 20-fold that level. We have no breakdown by year.

In the mid-sized corporate banking business, we were informed that there are c.6 companies going through probable exit processes, with 25 at risk of closure for a more complex list of reasons for which compliance risk/cost may be one.

In addition, the same bank provided information on closures within its wealth management/private banking business with 56 client exits for pure "risk management" reasons (associated with decisions by the AML committee) over almost three years from January 2013. 30 exits associated with SARS were noted over this period, but again the majority of these are likely to overlap with the 56. These closures were approximately evenly distributed across the three years. However, in addition to these examples, we were provided data suggesting that a larger number were closed in 2014/15 for reasons which did not include the same reference to the AML committee, but nonetheless may have related to compliance and reputational risk. Know Your Customer (KYC)[16] was highlighted in the majority of these cases. These latter types of closures took place at a much slower rate in 2015 than 2014.

4.5 Other Banks – General Remarks

We have selective qualitative data on account closures from a range of other banks. Of 18 other banks which provided some level of response to questions about account closures for AML- or financial crime risk-related reasons, only three said they had not been closing accounts for such reasons. Of the others:

- Two were in the process of reviewing their customer bases:
  - One bank in a low risk European country was not under direct pressure but wanted to avoid future issues with its interbank relationships
  - One small subsidiary was under direct pressure from its correspondents
- Two recent start-ups, UK challenger banks, were taking into account today's environment when considering which clients to take on in the first place and, in the case of one of them, rationing its number of highly cash-oriented clients given its limited compliance capacity.

[16] UK legislation does not refer to KYC, but many banks interviewed used the term KYC. The FCA Financial Crime Guide acknowledges that the terms may be used interchangeably.

- Two have had to reduce the service offered to existing clients (one small bank from the Americas, and one UK branch of an overseas bank).
- Three large UK banks (in addition to those above) have seen some AML-driven account closures. However, in these cases it is not always possible to distinguish between normal-environment AML closures and those relating to today's heightened sensitivities.
- Six others, all of them UK branches or subsidiaries of foreign banks, have indicated an increased level of account closures in the last one to three years.
    - In one case, a London branch of a large bank from the Americas, it exited its entire personal banking portfolio.
    - Another, a UK branch of a bank in a low risk European country, has cut 24% of its corporate & SME clients in 2014-5.

5 THE EXCLUSION COSTS OF DERISKING

FCA questions: The extent to which impacted customers have:

- *had difficulties and delays in accessing accounts;*
- *had accounts closed and needed to seek alternative arrangements;*
- *been financially excluded as a result of removal of banking services*

5.1 Issue of Definition and Data Collection

In this short study we were able to identify and contact members of the sectors in which the FCA were particularly interested. There are a number of issues that need to be born in mind when looking at the data collected.

First, we have on occasion in this report used the term 'victims' for those affected by derisking as, with hardly any exceptions, they felt they had been harmed by an event (here, derisking) which is consistent with the OED definition of a victim. The feeling of victimisation also flows from their sense of bank decisions to derisk being almost always made without them having any say in the final outcome.

However, when we use the term 'victims' we are not implying or judging that decisions to terminate, restrict, or not take on customers have been either justified or unjustified in the context of the current regulatory climate or their behaviour. In other words, some impacted customers may have 'deserved' their victim status; others may not.

SMEs tend to underreport incidence. Because of the perceived and actual damage done to businesses by the news that they have lost or been refused an account, or will soon, businesses are reluctant to speak out. The incidences reported here, which are by no means exhaustive, may reflect wider patterns of experience.

SMEs underreport costs. We noted that few of those reporting problems had considered the time involved resolving those problems as a cost or considered the opportunity value of the distraction caused. They were mostly concerned about the emotional impact of the hard and unjustified way, in their eyes, that they were treated and the uncertainty of continuing in business.

Minorities and vulnerable groups may complain less. We have not been able to establish the extent to which the distribution of personal customer complaints reflects over or under reporting in this respect.

We were not able to identify or talk to the discouraged. In addition to those denied accounts there are those who are put off before making an application, e.g. after reading the terms and conditions or talking to bank staff, or after talking to their friends, relations and others.

5.2 Interbank Relationships

Global correspondent banking is not a primary focus of our study. Recent reports by the Bank for International Settlements and the Financial Stability Board for the G20[17] have identified a contraction in the numbers of correspondent relationships globally. However, there are a range of relationships and transactions between banks which are being impacted by derisking. We propose to use the overarching term 'interbank relationships' to cover these.

5.2.1 Compounding derisking via the bank cascade

Many of the banks we have spoken to have indicated that, although they take a risk-based approach to each client relationship, they are not just building in the actual risk of a client (or its customers) acting in a damaging way – they are also building in their assessment of how the appropriate regulators, or financial institutions higher up the 'food chain' (who are almost seen to be acting in a quasi-regulatory capacity), will assess their approach. Essentially there is a certain amount of second-guessing going on. In today's environment, the vast majority of these assessments will fall on the side of caution.

To be more specific, one bank in a low risk European country has indicated that it is likely to (or has now already begun) closing relationships, including correspondents, in order to minimise the risk of difficulties with its regulator and/or its own correspondent relationships.

Also, several larger banks are sending medium or smaller banks lists of client types whose transactions they do not wish to process, or even those for whom they would prefer the smaller bank not to maintain an account. These lists include the high risk sectors identified as above, such as MSBs and gambling, and arguably constitute a form of wholesale derisking (by proxy) of client groups.

In one of these communications, there is also an indication of client types which the smaller bank is told to be especially careful with, though without absolutely proscribing relationships or transactions with such clients. We have not been able to raise this issue directly with the larger banks concerned. We suggest such letters with lists, which we have had sight of, are examples of the larger banks erring on the side of caution.

In turn, the recipients of these letters are likely to take an approach at the more cautious end of the spectrum in their dealings with banks and non-banks further down the chain, or even with their peers if they have interbank relationships with 'higher risk' peer banks. This compounded caution could be further exacerbated if there are further banks in the relationship chain. This doubly compounded effect could be studied using one or two large banks and their resulting relationship tree(s), and contrasted with examples of cascades headed by less risk averse banks.

5.2.2 Impact of cost of compliance

Banks have historically built a great deal of overcapacity into their interbank relationships, assuming that each incremental relationship provides extra cover or transactional options for minimal cost or risk. Now that each additional relationship is being costed in compliance terms, and in an environment where compliance expertise

[17] http://www.fsb.org/wp-content/uploads/Correspondent-banking-report-to-G20-Summit.pdf

has been bid up materially (see Section 6.1 for details), many of these relationships have been either pushed into loss, or at least are no longer seen as free, protective options. The overcapacity has therefore been rapidly disappearing. This is well catalogued on a global basis by the World Bank Correspondent Banking Survey, but can happen in other interbank relationships.

5.2.3 Impact on small and medium-sized banks and their clients

Of 26 surveyed small and medium banks, seven report having lost a material relationship with a larger bank, whether for UK clearing, correspondent banking, key foreign exchange processing, etc. A further seven report serious challenges, normally due to the impact of limitations imposed by a larger bank on whom they depend a great deal, or in one case due to repeated significant delays.

Three new domestic banks reported difficulties in finding a clearing relationship.

As alluded to in the 'Cascade' remarks above, several of these banks have reported closing some of their own relationships with smaller banks (typically respondents), due to a range of factors including: low revenues per relationship *vs*. high compliance costs; removing unnecessary overcapacity; self-censorship to avoid an impact with their larger peer relationship. Almost half have cut non-bank clients for similar reasons, while several are simply struggling to provide their clients with a sufficient range of services due to restrictions placed by their larger peer bank.

5.2.4 Data from large banks on correspondent banking relationships

At the end of 2015, a large UK bank had around 1.6k correspondent banking relationships. In 2015, year to October, this bank exited 78 relationships:

- 13 of these were due to the perceived risk of future financial crime, and another five were in some clear way compliance related – e.g. unable to provide crucial information such as KYC.
- A few closures indicated 'Dormant' or 'No relationship' but the majority of exits recorded a reasoning of 'Economics'.

In 2014 full year there were 66 exits:

- Five appeared to be related to the risk of financial crime, with another five relating to the inability to provide information.
- The majority of exits were of 'Dormant' accounts.

In 2013, there were 26 exits:

- Six appeared to be related to the risk of financial crime, and 4 were related to other compliance issues.
- The remainder were dormant or exited for reasons of 'Economics'.

In 2012, there were 37 exits:

- Six were recorded as being related to the risk of financial crime.
- The remainder were for reasons of economics.

The number of relationships opened in this period was not disclosed.

Table 5 indicates that another large UK bank has seen a steady reduction in correspondent banking relationships since 2011. We have no additional detail from this bank on this topic.

Table 5 Trend in a UK bank's number of correspondent banking relationships

Year	Y/e correspondent banking relationships
2010	c2.4K
2011	c.2.5k
2012	c.2.4k
2013	c.2.2k
2014	c.2.1k

A third large UK bank disclosed 1.4k correspondent relationships towards the end of 2015. It noted that 40 had been closed in 2014 as part of a review of correspondent banking relationships.

A global bank disclosed bank exits alongside closures of accounts held by non-banks. On this combined basis, the number of exits across the corporate and investment bank was at least 25 during 2013-5.

Another global bank has also closed a number of correspondent relationships, typically for a blend of reasons – non-core geography; replicating existing relationships; actual risk concerns. However, it has also been opening interbank relationships proactively in its core geographies, and training smaller banks in order to reduce its own transaction risks.

5.2.5 Example data from branches or subsidiaries of foreign banks

A UK branch of a foreign bank from the Americas indicated that it has cut most of its small number of correspondent relationships.

A UK branch of a bank from the Middle East has cut several of its peers in the region.

A UK subsidiary of an Arabic bank is in the process of reviewing its correspondent relationships.

The UK branch of a larger foreign bank has cut the majority of its 300 correspondent relationships having done a detailed review of profitability. Average revenue per relationship was previously around £30k p.a.

The UK branch of a large Asian bank has been approached to provide cash correspondent relationships.

5.3 Personal Account Holders

According to the Competition and Markets Authority (CMA)[18] there are more than 68 million active PCAs in the UK and 97% of adults in the UK have a PCA. PCAs generated revenues of approximately £8.7bn in 2014.

5.3.1 Issues with personal accounts

Personal account holders are the widest of the groups studied and the hardest to access directly in a short study. We therefore focussed on seeking data from organisations who regularly deal with personal account holders.

The data we obtained was almost exclusively about account closures. There were limited references to account opening difficulties and, as noted above, a key data need with regard to financial exclusion is the number of potential personal account holders who are dissuaded from even applying for a bank account. Those who do not have bank accounts generate the demand for cheque cashing facilities and cash loans from other sources.

5.3.2 Ombudsman Service

We approached the Ombudsman Service as it can help customers with complaints about most problems involving financial products and services provided in or from the UK. Its ability to consider a complaint depends on certain rules relating to e.g. activity, complainant eligibility and timeliness. For current purposes, this means that many derisking complaints do not fall within its ambit.

However, from a data collection point of view, the FOS's policy of encouraging consumers who believed they have been wronged to discuss whether they have grounds for complaint means it receives a steady stream of inquiries, including those regarding derisking. There are issues which take detailed analysis and interpretation of data on these inquiries beyond the scope of this study. However, some clear higher level issues emerge:

Casework teams estimate that that they deal with approximately 20-30 complaints per week about account closures due to AML/Proceeds of Crime Act issues. This estimate is based on the number of such complaints currently being worked on by the relevant casework teams and produces a crude annual rate of around 1,000 complaints.

Complaints relating to AML issues tend mostly to be about the *closure* of the account rather than a refusal to open one. However it is not clear if these complaints originate in changes in bank policies re standards and/or enforcement, or changes in client risk profile and/or activity.

As for the level of complaints itself, it seems plausible that people denied account opening might not consider it appropriate to complain to the Ombudsman service, or not know about its existence. It is not known if people who are refused accounts or closed down are routinely sent details of the Ombudsman service.

Complainants are not only upset about the closure of the account, but often also unhappy about the lack of explanation or communication by the bank to explain the

[18] *Retail Banking Market Investigation* Summary of Provisional Findings Report, CMA October 2015

reasons for the account closure. Many of them feel that they have been discriminated against because of their nationality.

5.3.3 Citizens Advice

CA operates nationally to provide the advice people need for the problems they face, whereby banking is a sub-category of CA's Debt and Money advisory work. CA aims to provide the right information about opening and running an account to help customers manage money properly and deal with any problems that crop up. This includes providing information on how to get a bank account, types of account available and switching from one bank or building society to another.

In the period 1 October 2014 to 8 November 2015 CA advised 3,936 clients in England and Wales about opening a bank or Post Office card account, 0.22 percent of clients advised in that period. CA's own analysis is that the majority of such inquiries relate to opening a bank account to deal with multiple debts.

Of these, amongst those with problems with bank accounts there were slightly more men than women and, in contrast to the popular narrative that these were likely to be people from developing countries, 80% were of White (UK or Other) origin. 4% were Asian/British Asian and 5% Black or Black British. Just under 80% were aged 20-59. Just under 50% were single or single with dependent children and the same percentage of clients had income of under £800pcm. 42% were employed and 19% unemployed. Again, minorities may not be reporting.

In the period July 2011 to November 2015 CA found 96 evidence forms on clients with bank account opening (63) and closing (33) issues. Problems opening accounts mainly related to providing proof of identity (POI) and proof of address (POA) and clients were often foreign or homeless or on benefits or used to having their affairs managed by others.

Bank rejection of POI for minor documentary issues was one cause of problems – e.g. a water bill not being considered a utility bill or 'Catch 22' situations where a person could not get a bank account to pay for their accommodation because they do not have accommodation. Box 5 (overleaf) illustrates the latter, which we regard as a form of derisking leading to reduced financial inclusion.

Box 5: Case Study from CA

Low or no income bank customers trying to open accounts can face large costs relative to their meagre resources. One of CA's clients was a homeless man with, by definition, no address and formal identification. Having obtained a job he applied to a bank account to receive his first wages. He was told to obtain a letter from his GP. This still meant him having to find the fee of £25 for a Doctor's Letter.

The requirement to produce two forms of official identity such as a passport or driving licence has no marginal cost for the overwhelming majority of customers who can afford to travel abroad and drive. But they can be significant and otherwise unnecessary costs of obtaining documents for those living on the margin.

A passport costs £72.50 and is not needed by someone too poor to travel abroad. A provisional driving licence costs £43 (*vs.* £34 for those with access to a payment card. Even renewals cost £14, plus the cost of photo and postage). In the context of a minimum national wage of £6.50 per hour these sums equate to between just under half a day to just under one and a half day's gross pay. There is thus a potentially regressive effect in the fixed costs of POI on poorer customers.

Similarly, those who are poor often live with friends or relatives so they do not have utility bills in their own name. However, issues of unwillingness to accept alternative forms of POA arise in the same manner as refusal of alternative forms of POI.

The CA also noted account closures related to a) nationality or the country with which an account holder did business (notably Iran) and b) being the *victim* of fraud, though the data presented above do not show this explicitly.

5.3.4 Other incidences

We also came across private individuals who had had their personal accounts closed because they were related to business clients in consumer credit who had had their accounts closed.

The prevalence of complaints about account closure as opposed to account opening may not be surprising – people are arguably more likely to complain about the withdrawal of an entitlement as opposed to the refusal to grant one in the first place.

But we also note that each withdrawal of a business account usually creates multiple subsequent rejections of applications for an account. Those looking for alternative accounts run up against the same objections as led to the initial account closure and the fact they have had facilities withdrawn by another bank can count against them in

subsequent applications to other banks. Amongst those we talked to such applications rarely succeeded.

5.4 FinTech Sector

The UK is a leading, by some standard the leading, financial centre in the world. It thus has an interest in encouraging new FinTech companies in, and attracting them to, the UK, as well as promoting their role in and from the UK once established. Accordingly, the government wants to 'assist more companies looking to establish a presence in the UK; and help both indigenous and foreign owned UK companies leverage opportunities internationally'[19].

The spectrum of technology termed FinTech covers a wide range of activities from payment systems to analytics, risk and accounting systems to trading platforms. One 2014 report estimates the value of the market for which firms in the UK compete at £20bn, of which just under a fifth is accounted for by emergent FinTech, a sector where UK accounts for around half European start ups.

From a derisking perspective there are two key considerations. First is the question of the risk profile of FinTech companies from an AML/CFT perspective. The possibility and reports of proven cases of illegal payments through both novel payment systems and companies with novel underlying technologies has led to reluctance to provide banking facilities in this area, even though the NRA rated new payments methods (e-money) as a 'Medium' risk and digital currencies as a 'Low' risk for money laundering. However, the drivers of demand for new systems and technologies arise in part from the dissatisfaction of bank clients with existing products and services.

This in turn leads to the second consideration, namely that vested interests play a role. The narrative here is that reluctance on the part of some banks to invest in or bank certain types of new technology is because they might rival their own products and services, or because banks wish to gain control of such technologies for themselves by manipulating access.

Competition issues were indeed raised as possible motives for derisking by some respondents. In this report we focus on recounting the experiences of FinTech companies involved in payments systems or using certain technologies, as this is where there were most reports of issues arising. We established that the EMA had already been in contact with the FCA on this matter so we reviewed their submissions and talked to a number of its members.

EMA has 44 members, including famous names such as Google and Facebook as well as start-ups. In 2012 its members had 85m customers and processed 1.3b transactions worth E43.6b. In March 2105 the EMA described in a letter to FCA the decline in ease of access to accounts over the previous 12 months among members with different business models, client bases, products and risk profiles. Derisking policy was cited by the banks as the reason for account closure or refusals to open accounts.

The EMA suggested there seemed to be a view that EMI/PIs are particularly risky clients, though no particular business type triggers this sort of situation. The phenomenon did affect companies providing financial solutions to the underbanked population segment, e.g. money remittance companies serving migrant workers,

[19] Landscaping UK FinTech A Report by Ernst & Young Commissioned by UK Trade & Investment 2014

debit/prepaid card issuers, ATM and POS acquirers, and companies dealing with gambling services.

The refusals were mostly by letter, without reasons being given or any potential remedial action offered. Sometimes staff suggested informally that their bank did not deal with EMI/PIs as a general policy. The banks involved were both first and second tier, UK and foreign.

EMA provided three examples which are set out in Box 6.

Box 6: Case Studies from EMA

Company A (EMI: Platform technology, voucher and smartcard payments including gaming and gambling systems).

In 2013 Company A was refused an account without further investigation into clients/ or risks, on the grounds that its stated annual turnover of EUR10m was not satisfactory, and the non-UK nationality of the Director and 100% shares owned by non-UK UBOs did not satisfy Bank A's due diligence requirements.

The company were told by external advisors in the UK that it was not practically possible for a newly established EMI to open a bank account. The company relocated to a different EU member state, where it now operates.

Company B (Authorized EMI and Principal MasterCard member. E-wallets, issuer of MasterCard debit/prepaid cards. Broad range of risk profiles, mainly UK/other EU).

The company was given a 60-day notice of closure by Bank A for 'risk management' reasons. It has had no success in the past 12 months opening office and client safeguarding accounts with the UK banks. Bank B agreed, and then reversed its decision, again specifying risk-based reasons.

Unofficially, they were told head office policy did not allow bank accounts for prepaid card issuers. The firm had other applications pending, one for eight months, supported by the local branch. No response was received to requests to banks to specify remedial action that would permit an account to be held.

The company has been trading for over 10 years without experiencing any instances of credit or overdraft facility use, AML issues or security breaches and does not deal with cash or cheques. It is not perceived as a risk by Tier 1 banks in other countries.

Company C (Online payment processor. I-gaming and internet casinos located throughout the EU)

In the four months to March 2015 it experienced closures of three bank accounts used since 2007 with Bank G, Bank H and Bank I. No statement was given as to how bank concerns could be addressed. It was also unable to gain access to a bank online payment solution. One bank stated explicitly that it will not make its online payment service available to a PSP providing its own online payment platform/service.

We talked to another member, Company D, which is licensed as an E-Money issuer and wants to provide alternative bank services for SMEs. They target the gap they see created by 4MLD, Payment Services Directive (PSD) and other regulation between money issuers and full banks. They would fill this perceived void by providing alternative bank equivalent services under one regulatory wrapper. They are working on a model where they would hold client funds and act on agency basis providing direct debit, credit and card facilities.

They obtained a degree of co-operation with some departments of Bank A, being taken into its innovation hub and even introduced to SMEs Bank A had derisked. However, they experienced Bank A operating in silos and, despite presenting to the risk committee, for each pace forward they also seemed in the end to move one back. A year later, they are still not at transaction stage. Another bank they approached wanted $24m collateral for card operations, out of proportion to proposed trading volumes.

This company also knows of other FinTechs that have been offered £ Sterling and Euro accounts but not a US$ account. It said the sector assumed a blanket ban on Bitcoin type operations and that members doing MSB business had had their accounts shut down or were told to stop.

Another FinTech company was refused facilities because it had a block chain based technology for improving the integrity of the market in gemstones. They, like other players in this area, felt there is a lack of awareness in banks, regulators and law enforcement about the upside and downside risks of new technology, which negatively affects views of E-Money, prepaid cards, and anonymous payment systems.

FinTechs also feel there is limited appreciation of the higher quantity and quality of data they believe they can access, especially compared to banks doing CDD following traditional POI and POA approaches. The basis for this feeling seems to be the FinTech companies' perception that they are better equipped technologically to undertake investigations into individuals and transactions using open sources. There was no mention of access to criminal intelligence being an issue with their CDD efforts. Rather they saw themselves as being well placed to contribute to such processes.

The fear among FinTech companies that access to banking is no longer assured was echoed by the DCA. It reported that, at one point, banks were not offering facilities to conference companies and others servicing, but not involved in, digital currencies. Their case studies have been shared with Her Majesty's Treasury (HMT). Again, Bank A's innovation arm had shown more flexibility than other areas of the bank. Where digital currency operations were in some way linked to remittances there were big problems. Moving away from a larger bank did not resolve these issues as smaller banks use larger banks as clearers and the same issues remerged at clearer level.

Bank E was approached by one DCA member for its 'agency banking' facility, but this has now been closed by Bank B (which provides agency services for non-clearing banks, one of which was Bank E).

5.5 Money Service Businesses

With FCA agreement, the fieldwork for the Study has not focused on the MSB sector to any great extent. The sector, in particular the subsector involved in money transmission activities, has been widely surveyed (most recently at a global level by the World Bank on behalf of the G20) and has also been amongst the most successful at highlighting the

problems of losing bank accounts. The decision by certain UK banks to close a significant proportion of their MTO accounts in 2012-13 and subsequent legal action taken by Dahabshiil and others is sometimes seen as marking a watershed in the derisking debate, bringing it to public, political and regulatory attention. Concerns about the potential humanitarian catastrophe of global restriction on remittances have made up a substantial part of the narrative on derisking impacts.

It is clear from the evidence that many small MSBs have had difficulties with their banking arrangements and more regard their situation as precarious. Many have felt pressurised to change their business model, for example becoming part of larger networks, despite their own beliefs that their compliance arrangements were superior (based often on greater personal knowledge of customers) to those large firms. They regard this as a commercial decision by banks, with AML/CFT issues used as an excuse.

The NRA rates MSBs (in all guises, not just MTOs) as a 'Medium' risk for money laundering, but 'High' for terrorist finance. However, transfer of criminal funds overseas and third party payments (used by some MTOs) are highlighted as specific money laundering threats and vulnerabilities to the sector.

However, what is less clear is the actual overall impact on the sector. Some firms may have gone out of business, some operating under different guises and some undoubtedly 'flying under the radar' (and therefore at further risk of de-banking should they be discovered to be using personal or other business accounts for MTO purposes), but there is no broad and reliable data on the impact on underlying remittance flows.

The evidence in the UK suggests a small, possibly single figure, number of firms that have gone out of business as a result of losing their bank accounts, but a much larger number who have suffered closure and/or difficulty opening accounts. The data can be interpreted in a number of ways. Most surveys in this area have had a relatively low response rate. It appears that the sector is under stress, but it is unclear if it is fatally affected. One possible outcome is a sudden implosion of these businesses as they run out of working capital or become unprofitable. Another is that they become agents of larger companies at much reduced profitability to their owners. They may or may not engage in unofficial MSB activity at the same time or as an alternative.

An illustration of the problems faced by companies in this sector is given in Box 7 (overleaf).

Box 7: An MSB Case

Company E, which is also in consumer credit and pawnbroking, was told by its bank that it should no longer offer its own FX service. It has the option to continue as an agent for another (bank-approved) provider, but the bank might well change its position (negatively) in the next 3 months

The company had been using another company as wholesale currency provider, which was also told by the same bank not to offer wholesale FX to MSBs on pain of losing *its* account. In effect Company E is having to become the agent of bank mandated companies for money transfer, third party cheque cashing and FX. As it is technically no longer a MSB, the bank won't be accused of closing the account for MSB reasons, if it does eventually close it.

It was told that any provider, for whom it becomes an agent, must be a customer of the bank. It will lose approximately £60,000 in revenue annually by becoming an agent for bank approved FX services and has lost £70,000 in revenue after having been forced by the bank to become an agent of a bank approved check cashing company. These are significant sums for a small-medium sized business.

The company feels there has been no attempt on the bank's part to apply proportionality, due diligence or common sense when making these decisions. It does not feel treated fairly treated.

5.6 Financial Services for the Unbanked

5.6.1 Issues with personal credit

Personal credit plays an important role in supporting those who, in the main, are unable or unwilling to access mainstream credit sources and live on the margin. These individuals are easily pushed into debt by events most people can cover, e.g. periods of unemployment or between seasonal or agency contracts; Christmas and summer holiday costs; and essential home appliances. Historically, pawnbrokers and home credit businesses also offered cheque cashing and, in the case of pawnbrokers in recent times, money transmission services.

Home credit and pawn broking have historically provided one alternative to those loan sharks and unscrupulous doorstep lenders whose rates of interest and approach to recovery can have catastrophic outcomes for those whose are often vulnerable – single mothers, long-term disabled. Some small business and the self employed have also turned to personal credit when banks stopped lending to them after the 2008/9 crash.

This is a longstanding sector with geographic concentrations in poorer regional areas notably the West Country, Midlands and North West. A high value pocket exists in the Greater London area. We focussed on the smaller end players where there was more evidence of derisking.

5.6.2 Pawnbroking

We obtained a number of detailed case studies from the National Pawnbrokers Association. These highlighted long term sensitivity of the banks to pawn brokers' involvement in cheque cashing and more recently in MSB activity - 72% of NPA members are MSBs.

A survey of its members in September 2015 (295 members, 76% response rate) demonstrated the impact of business current account (BCA) closures on the pawn broking industry across the United Kingdom. 41% of members had had an account closed. The percentage of accounts closed by banks is shown in Table 6:

Table 6 Percentage of Accounts Closed by Bank

Bank	Accounts Closed (%)
Bank	33.0%
Bank	23.1%
Bank	20.9%
Bank	7.7%
Other	15.3%

As a group, NPA members were highly dependent on two banks that provided just under three-quarters of all bank accounts. Any such duopoly would necessarily have impacts in terms of competitiveness and business continuity risk should either or both of the providers withdraw from this type of business.

Table 7 Market Share for All NPA Respondents

	Primary Current A/C	All Accounts
Bank A	(91) 41.6%	(104) 40.6%
Bank L	(83) 37.0%	(86) 33.6%
Bank N	(16) 8.5%	(25) 9.8%
All Others	(34) 15.1%	(43) 16.8%
TOTAL	(224)	(256)

Table 8 Market Share for NPA Respondents who are also MSBs

	Primary Current A/C	Other Accounts	All Accounts
Bank A	(69) 42.9%	(12) 50%	(81) 43.8%
Bank D	(74) 45.9%	(2) 8.3%	(76) 41.1%
Bank B	(7) 4.3%	(7) 29.2%	(14) 7.6%
All Others	(11) 6.8%	(3) 1.2%%	(14) 7.6%
TOTAL	(161)	(24)	(185)

91% of MSBs only had one current account with no back up account. Therefore these members are most at risk of total debanking.

Table 9 NPA-Member MSBs Primary Account Banks Holding the Only Bank Account

	Primary Current a/c	Only Account %
Bank A	(69) 42.9%	(57) 83%
Bank D	(74) 45.9%	(72) 97%
Bank B	(7) 4.3%	(7) 100%
All Others	(11) 6.8%	(8) 73%
Total	(161)	(144) 89.4%

Pattern of Closure

The pattern of account closure appears to be that one particular bank was first to exit the sector based on its judgment initially of the risks posed by cheque cashing businesses and later of the MSB sector. Another large bank then made a big push into the sector before the global financial crisis, only to start pulling out two years ago. NPA members say one bank has stated that it has no wish to be involved in the MSB or Pawnbroking sectors.

Pawnbrokers do hardly any cheque cashing now because of worries about losing their accounts and are now halting MSB business for the same reasons. One NPA member

advises that he was told to stop all MSB activity by Bank A. The pattern of closure is similar to other areas, i.e. a call giving 60 days notice out of the blue or continual requests for data and to desist from certain lines of business followed by closure.

One NPA member had its account withdrawn in 2012 with words to the effect of 'the cost of compliance for your sort of business is so high that we would have to charge you £25k for you to keep the account, so we are going to close it'.

Impact

The NPA survey found competition adding to choice in metropolitan areas but leading to severe pressure on regional independent members down to the last bank account. It sees a tangible risk of independent members being forced out of the market by debanking over the next 24 months leaving a small number of large multiples dominating the market and limiting consumer choice across the board.

In metropolitan areas high street bank presence has been reduced in areas (DE and C2 Demographic Groups) with below average access to financial services, including alternatives such as credit unions. Pawnbroking appears to be one of few legitimate and responsible forms of financing for some of these types of urban areas. The NPA believes any reduction in service provision might favour multiples and encourage illegal loan activity.

In rural and market town areas, any reduction of provision will have a direct bearing upon peoples' livelihoods. For example, if local pawn broking stores Cornwall were closed, the nearest provision for someone in Penzance would be located in Plymouth in Devon. NPA estimates that the closure of pawnbroking stores in rural areas and market towns could lead, on average, a journey of approximately 20 miles to seek alternative provision. For people of some income groups, the immediate cost of transport would make such options unrealistic.

NPA reports that in Northern Ireland, it has been advised of the continued prevalence of illegal consumer credit activity in parts of the province undertaken by individuals who were linked to former paramilitary groups on either side of the sectarian divide. NPA says pawnbroking is not advanced across all of Northern Ireland, but is still often the only legitimate and regulated provider of short term finance for some people from D, E and C2 demographic groups, as credit unions in are still at an early stage of development. The closure of pawnbroking operations, which are primarily independent businesses, would have a disproportionate impact on, especially, low income people in Northern Ireland compared to the rest of the UK.

5.6.3 Consumer (Home) credit

Of all the sectors we approached, we received the most immediate and direct response from small and medium sized home credit businesses. Box 8 sets out a case which represents well the dozen or so calls we received.

Box 8: Consumer credit case

Company R is a door step credit business in a mixed urban and semi urban area. From 1971 it banked with an entity which became Bank C. It had no real contact with the bank prior to 2012, even when doing weekly cash paying-in runs. All administration, such as the overdraft facility renewal, was done by post without any discussions.

In Q2 2012 the owner was asked to an interview. Ways of refinancing its borrowing (loan to surety ratio 1:9) were discussed with the owner offering to clear it by the pending sale of a property (the owner lives in UK and in an EU holiday resort area). At the start of Q3 he was called by mobile phone whilst on holiday and told his business accounts would be closed by end Q3, by which time he should clear all outstandings or face legal action. The firm was OFT AML registered and fully OFT registered.

Informally the bank said it wished to 'disassociate itself from this type of business'. The owner's personal account was not closed and some standing orders were transferred to that account by the bank – ones associated with products the bank had insisted the owner take on, such as critical illness cover at over £1,000 p.a., as a tacit condition for a loan to buy the business from his father, the previous owner, twenty years or so earlier.

The owner received numerous warnings to ensure all was settled on time in the run up to closure on pain of legal action. He was advised to try Bank A which he did but never heard back. He closed these accounts and operates by other means. He reckons he will exit the business soon given the problems and uncertainties.

The pattern of sudden termination of viable businesses after years of indifference or neglect on behalf of the bank is a recurring theme at the smaller end of the sector. It is characterised by long standing second or third generation businesses being forced out of the commercial areas of banks, but in some places tolerated or unobserved when owners continue using other relationships with banks. It begs questions as to how the banks involved have been looking at risk and CDD. Ironically, those doing business where they can without business bank accounts save transaction costs, but at the price of uncertainty as to whether they will run into problems for adopting other approaches.

We also came across medium sized businesses with high street outlets and 65-75 employees who had either lost their accounts or where at risk of doing so. The conditions placed on one firm which had not lost its account are reported under MSBs. Among these firms were many expressing the concern that a desire to operate in some parts of this sector, on their own account or via associated companies, was a possible motivation for bank derisking behaviour.

One such business had been told that, were it turning over £30m p.a., it would not be having business account problems. It pointed out to us that this level of turnover and above was the realm of pay day lenders who had been fined for not treating customers fairly, which micro-lenders needed to do in a market where location and reputation were key. It also felt it knew its customers for CDD purposes much better than the banks. It saw the banks as gaming FCA derisking advice, whereby the 'commercial

decision' justification provided a convenient, non-recourse means of terminating any relationship which banks thought might get them into trouble. The sector, they stated, was being 'discriminated against' with banks failing to properly assessing risk. Given the transaction sizes involved and lenders' knowledge of a client base of mainly vulnerable and financially excluded individuals, they thought the scope for serious abuse was low. The firm operates across rural and urban areas.

A business which had its accounts closed employs people in the North West. Established more than eight years, it is the successor to another successful similar company with £350K profit per year and 8,000+ clients. It banked with Bank B being always in credit, with c. £40K in its business current account and £200K +/- on deposit. It ran its own AML/CFT systems. It was never visited, or had its systems checked, by Bank B and claims never to have had any complaints them.

In mid June 2015, it was given until mid-August to rebank in a letter that said there would be 'No Discussion'. After a month's grace they were debanked in September by being sent a cheque. With no bank account to pay it into they ended up taking cash.

With no account they also cannot get a card payment system to allow crediting and debiting of clients which their clients often prefer (benefit is paid into client card accounts). They are running on cash but can't sustain such operations. They are facing collapse and have approached other banks, getting local level support and national level rejection, which appears to be a pattern among those we interviewed. Bank F recently visited and said it did not take a sector based view as other banks did. However, nothing had yet been heard from them. The company fears loss of jobs and illegal operators moving in to fill the void they leave.

We encountered similar stories to the above across England and Wales including the West Country, Potteries, Yorkshire and Greater London area.

Among those who had lost their accounts there was anger at how viable businesses were being marginalised or pushed under, as owners saw it, to the detriment of them and their clients, some of whom they have known across generations. Those who still operate by other means say any savings in bank charges are offset by uncertainty.

In all cases there is anger at how the banks, having encouraged them in one direction, have simply changed their minds and been, as the banks see it, brutal in doing so. As micro-lenders they are very 'high touch' in their approach to their own businesses and wonder how bankers can be so offhand in theirs.

These statements have to be balanced by the observation that there are some people to whom home credit lenders choose not lend. Universal banking does not imply universal credit.

5.6.4 Issues around alternative banking services

Based on UNITE/European Commission figures for April 2015, NPA suggests that 9m adults in the UK do not have a bank account and therefore are those most likely to rely on pawnbrokers and MSBs for transactions. It says most people in the UK require foreign currency at some point and the non-banking sector generally offers better rates for foreign currency, access to money transfers. Pawn loans are generally cheaper than equivalent short term bank lending (BBC Moneybox from 2011).

It is not clear where these 9 million citizens, who include those not interested in or put off from having a banks account as well as those derisked, would go for their financial transactions if those offering alternatives to banks have their accounts closed. They either face the higher cost of services from businesses that stay open or fall prey to the illegal operators – for example having to choose between loan sharks and the 'pay day loans' sector. As the pressure on the latter to derisk increases, opportunities for the former increase.

If all pawnbrokers/MSBs closed, the NPA argues that up to £5bn finance would have to be found from another source. As mentioned above around 10% of pawnbroking stores are in rural locations. If these closed it could have a devastating effect on rural and other communities affecting around 1 million people. Wales, N Ireland, parts of Scotland and SW England would be worst affected. We found that lending in both areas tends to be for sums of £100-£1,000 (though there is a higher value market in big cities) and APRs are around 240%

5.7 Defence and Security

5.7.1 Background

There are various figures for the global defence procurement market. One leading professional service firm estimates 2014 level at $86bn rising to $93bn in 2018.[20] According to *Stockholm International Peace Research Institute* (*SIPRI*), in 2013 the UK was the world's sixth largest arms exporter, with military exports making up about 1.5 per cent of total UK exports, and arms export employment accounting for 0.2 per cent of the workforce (Campaign Against Arms Trade (CAAT), 2011).

Like other markets the defence sector creates demand for a wide range of financial services and both UK banks and foreign banks in the UK openly advertise their skills in this area (e.g. Bank A and Bank J). The sector provides interesting investment opportunities as well as the prospect of transaction fee income.

However, the provision of banking services to the defence sector presents a range of informal and formal regulatory challenges which can influence the decision to offer or maintain banks accounts.

The defence sector facilitates the formal legitimate defence of national territory, citizens and interests. However, it has historically been, by its very nature, the subject of social and political controversy over the sale and use of its products in particular circumstances. These concerns are longstanding and based on well known principles and for some clients of financial institutions the mere production of weapons is abhorrent. This is an incentive for financial institutions not to bank the defence sector.

There has been an increase in export controls relating to the sale and financing of arms, especially landmines and cluster weapons, as well as the illegal sale of arms and components to certain countries embargoed by the wider international community. However, the sale of defence equipment is highly regulated in the UK, and financial institutions have to know their way around these rules.

[20] Global Defense Outlook 2015 Defense and Development, Deloittes

All these factors create further levels of concerns, checks and balances. In addition, some goods may be dual use, i.e. deployable in peaceful and conflicted environments which financial institutions need to be able to recognise if they are to react appropriately. The historical lack of transparency evinced by players in this sector simply compounds the situation.

As a result, many large financial actors follow some form of criteria when providing services to clients in the armaments and defence sectors.[21] The key lies in balancing safe banking controls with the need to protect of domestic firms who have an important defence role. Small firms are particularly vulnerable as the cost of monitoring them is not offset by greater opportunities for fees. Also, knock on effects in the supply chain mean that the effect of derisking of small companies is not limited to that company, and may impact large multinational collaboration projects – a key feature of many large defence projects.

A further consideration is that, whilst the number of small companies is getting ever smaller, small companies are often some of the most innovative, and global defence R&D budgets are an important target for UK defence SMEs to target.

5.7.2 UK experience

There has been significant work done on this issue by government and trade organisations. A survey of members of the defence industry, in 2014, received around thirty responses from companies who had had banking issues. Those involved in munitions and maritime security seem to be predominantly affected.

An evidence-gathering workshop was held with Defence SMEs and representatives from BIS and Ministry of Defence (MOD) in May 2014 in which two common themes emerged:

- **Access to banking services**: banks appear unwilling to providing banking services to Defence SMEs particularly those involved in munitions, on ethical grounds (though the ethical grounds are plausibly related to reputational risk). Without access to a bank account the logical end point will be for UK companies to close down or move their operations abroad, with a subsequent loss of jobs and sovereign capability.
- **Support to exports**: banks are sometimes unwilling to support letters of credit/export finance, despite an SME receiving an export licence. This problem appears to be affecting not just munitions companies within the defence sector.

[21] Research Paper Elli Kytömäki International Security Department | December 2014 The Defence Industry, Investors and the Arms Trade Treaty

Typical problems encountered included:

- A ballistic test equipment manufacturer whose equipment is widely used by MOD and many suppliers to MOD. Their accounts were closed with 60-days' notice, extended by an additional month after an MP intervened. It applied to open accounts with 4 other banks but applications were rejected based on of the company's trading sector as was the original closure. It struggled to obtain banking support for export deals e.g. an order from Indonesia worth US$4.9m that has United Kingdom Export Finance/Export Credit Guarantee Department (UKEF/ECGD) support and a UK export licence, in relation to which no UK bank is willing to provide assistance on any terms. The company negotiated with an Indonesian bank based in Singapore to solve the issue.

- A company specialising in the design and manufacture of specialist video surveillance equipment had its balances reduced to zero - as were the personal accounts of several company directors. Three weeks' later, the funds were returned to the accounts without any explanation. The company was subsequently issued with a 60 day notice of account closure by one of its two banks. Several weeks later, the company was also issued with an account closure notice by the second. No explanations for the account closures were received from either bank. Ironically, it subsequently got banking facilities with a third bank known to be very much against giving accounts to defence sector firms.

- A large multinational systems manufacturer and integrator won a US$16m order to export anti-tank weapons to Indonesia and duly signed a contract with the Indonesian MOD. When the MOD raised the letter of credit, the company's house bank rejected it without informing the company. The company was forced to rearrange for the letter of credit to be advised through another bank: a process which took six months and forced the company to miss key end-year deadlines.

At the time the industry's view seemed to be that these problems resulted from banks derisking and that it was a structural, regulatory issue. Following the workshop, the industry worked with Government to establish a defence and security forum with the BBA to increase communication between the two sectors.

We did not receive reports of any further cases in 2015 and the situation does appear to have stabilised. The issue will be followed up by industry in the course of 2016 to establish how conditions are then.

There are two main approaches. In some countries, there is a list of arms companies who produce banned goods. Banks may not deal with them by law (e.g. Belgium). In the UK strong trade bodies and official backing from MOD seems to have had a short term positive impact (especially dialogue with BBA), which appears to be an example of where dialogue works.

5.8 Charities

In its report on charitable giving in 2014 CAF reported that 70 per cent of respondents to its survey had given money to charity (either directly or through sponsorship of an individual) in the prior 12 months. The estimated total amount donated to charity by UK adults in 2014 is £10.6b. Based on Charity Commission data on prior years, adding legacies, endowments and other income to personal giving would produce a total

voluntary income figure two-thirds or so higher passing through charities books and bank accounts.

Medical research had the largest proportion of donors (33% in 2014), followed by 'children and young people' (30%) and 'hospitals and hospices' (25%). 'Overseas causes' accounted for 20%.

'Religious causes' achieve the largest share of donations in terms of total monetary value (14%). Cash is the most common method of giving (55%) with direct debit the second most popular (30%), followed by online giving (15%) and text (11%).

None of this would be possible without the use of banking facilities, whereby the importance of cash, the prevalence of religious charities and geographic areas in which charities operate all have the potential to trigger AML/CFT concerns. The NRA stated that although proven terrorist abuse of the charitable sector is rare, the terrorist financing risks within the charitable sector are medium-high. The impact of this somewhat opaque conclusion has yet to be understood, but it is unlikely to lead to greater willingness to retain or take on charities.

We asked a range of larger and smaller charities to describe the problems they faced themselves and the problems they thought other charities were or might well be facing.

Origins

There was a common view among charities that the current, derisking, phase of the problem had been going on for at least 4 years. Prior to that, the introduction of FATF SR8 had already led to an increase in CDD requests from longstanding banking partners, including lengthy reviews of management procedure and business models.

Top 'household name' charities are not derisked, but small charities are, and we talked to one which had lost bank facilities suddenly because of its area of operation (S. Sudan). It was only able to operate on a cash basis and was having difficulty paying staff. This type of event reinforced the charities view that the matter was now no longer one of cost of, but access to, banking services and thus existential. There was a fear that an avalanche of derisking in the not too distant future that might affect hundreds of charities – CAF has 1,250, of which the overwhelming majority are smaller institutions.

Impacts

We were not able to establish a conclusive number for charities who have lost accounts or who have had to alter their type or area of operations. We met charities operating in conflict countries who have been particularly hit, especially those who exist to respond to emergencies where speed of response is of the essence (e.g. where a natural disaster occurs in a conflict area) and clearing payments takes longer than 'golden response time'. The CFG, which has more than 2,300 members managing more than £20bn in charitable funds, has been active in the derisking debate. However, both they and CAF report that trying to establish the number of charities losing accounts is difficult, as the charities that have suffered tend not to want to admit it for fear of jeopardising other current or future banking relationships.

We also heard from some charities that the way banks approach ML and TF risk may create risks to life and limb for their staff, who are in danger if there are restrictions placed on how and to whom they can give money. We are not talking here about the

freedom to give money directly to known terrorists but the ability to distribute aid monies using local systems which may inevitably pass through areas controlled by terrorists. We are also talking about maintaining aid flows to areas where the recipients may resort, out of desperation, to aggressive measures against aid staff.

Charities have also encountered specific direct costs of obtaining legal opinions in order to maintain bank account facilities. One famous name charity required £40k of advice on sanctions regimes in order to maintain operations in a number of jurisdictions. It, like other charities, has had to invest donations in upskilling what used to be clerical level staff in its treasury department in order to deal with policy issues and complex requests for information from banks. It also has to spend money corroborating its position regarding its submissions to banks.

The impact on operations is to create unpredictability or delay (e.g. through need to pre-clear transfers). In addition there is the distraction (opportunity) cost – one leading charities group explained it is hearing constant concerns from members on AML/CFT issues at a time when charities face other pressing problems.

Aggravating factors

The charities we spoke to suggested that some of their problems and associated costs were due to a lack of coherence between government departments, sensitivity caused by internet noise and social chatter, and unnecessary pressure from banks as a result of these factors, especially when they were reflected in CDD databases whose perceived authority was on a par with the volume rather than the quality data in them.

Charities also thought banks had been sensitised by the few bad eggs that had slipped through the net and were using the commercial decision excuse as a blanket way to avoid that happening again. Communication was also an issue, whereby charities feel banks spend more time watching each other and trying not to be the ones who derisk a charity's last account – the last to derisk gets the opprobrium. On the other hand, some charities we did talk to described their banking arrangements as consisting of a primary account, through which most of their funds may flow, and one or more secondary accounts with lower amounts of transactions. They thought banks should talk more to charities and develop a shared approach to risk.

As with businesses, charities are seeing that a refusal/derisking by one bank compromises approaches to other banks. They were concerned that the sector would consolidate into big 'safe' charities with high overheads, and the exit of smaller specialist ones. This would not appeal to donors who value direct giving, meaning unofficial, often cash, charitable flows would increase.

The big charities thought that as it was bad enough for them, smaller ones would be hurting even more. They acknowledged that charities might not necessarily be more questioned than commercial players but they had fewer resources to respond. It was getting worse as the questions asked reach down to small repeat transactions.

5.9 Other Sectors Possibly Affected

Whilst we understand the following areas are not the FCA's main areas of concern, we include the following groups where we found anecdotal, actual or implied evidence of barriers to account opening, as this might be helpful in developing a comprehensive policy to derisking.

5.9.1 Diplomatic and other government staff

Among public sector workers, we heard from a government source of problems faced by UK crown and civil servants who are posted abroad and later refused accounts by UK banks or incur higher charges for banking products and services. The overall number potentially exposed is of the order of 10,000 and the number potentially affected at any one time about half that. They include FCO and DFID staff, who may spend half their careers abroad, and MoD, police and other public sector employees posted abroad for fixed periods.

These individuals have problems because they can be refused accounts on one or more of the grounds that they are domestic PEPs, even though that is not the case, that they have lived in specific countries, or that they have no (or an interrupted) credit history in the UK[22]. Some are required to serially remortgage their properties according to whether they are based in or outside UK and may have to approach specialist lenders who charge higher rates - up to 5% higher according to one report.

It is deeply ironic that not only are these individuals mostly those subject to strict security checks according to their grade and specialisation, but that they include some of those engaged at the heart of efforts to address the very threats AML and CFT regulation is designed to tackle.

This phenomenon is sufficiently common that the FCO itself has looked at it in detail. It would be surprising if this form of derisking is what was intended by FATF as implemented via 3MLD, as opposed to the case of officials serving abroad who are may validly be regarded as PEPs by local banks. However, 4MLD *potentially will* bring some officials within the scope of AML/CFT as domestic PEPs, so the problem is still a very clear and present one.

We have approached the Dean of the Diplomatic Corps in London to compare the situation with public officials posted to UK and await a response.

5.9.2 Students

The big UK banks offer university students special bank accounts and inducements to open them. Most students are happy with their accounts, which they tend to open with banks where they already have accounts, but one-third do not open accounts with existing relationship banks.[23]

Though students have on average shortfalls at the end of each month of £265[24] we encountered no reports of bank account closures – just overdraft limits being reached and further debits blocked. The problems of which we did hear mainly affected foreign students opening accounts. At one university the requirements were as follows:

- Bank F: University student ID card and passport. No need for supporting letter from university.

[22] We also heard of military personnel having problems relating to incomplete credit history but were unable to investigate these claims further.
[23] Save the Student (A student money website)
[24] Ibid

- Bank A, Bank C: Passport and university letter. International students with a visa for less than 12 months not eligible. PO Box number home address not acceptable.
- Bank D: Passport and university letter. Tier 4 Visa holders only. No PO Box home addresses.
- Bank B: Passport and supporting letter, (addressed to you). Courses of 6 months or more in duration. No PO Box number home addresses.

At another university the situation is essentially the same, with Bank C also requiring an original document/letter issued within last 4 months to the applicant's UK home address. UK undergraduates must also include their UCAS track letter. International Students are sometimes required to open a basic bank account in the first instance and then they can switch to a standard international student account after 6 months or so. They may be subject to higher burden of proof of income.

The issues here seem to be ones of ID, which may have AML/CFT reasons (e.g. money mules), and the cost of account opening. Again this strict application of standards relating to CDD is a form of derisking. We approached the NUS in London and await a response.

5.10 Closing Observations

We close with two quotes from people who have been derisked.

'I have stayed in this business because I know we help people who are marginalised and have very few options. These are customers that in many instances are unbanked, or underbanked. The irony is, the bank doesn't even want their business, and because they aren't a customer of the bank, the bank can't be accused of treating them unfairly. However, the banks are tacitly doing just that with every unjustifiable decision that negatively impacts a retail financial services provider'

An MSB Owner

'The net effect of policy is to transfer risk to those least able to absorb it and exclude those well placed to develop risk mitigating solutions….'

A FinTech Owner

6 THE COSTS OF TRIAGE

6.1 For Banks

FCA questions:

- *the costs of onboarding individual customers*
- *the costs of enhanced due diligence for customers with a higher risk profile*
- *the costs of ongoing monitoring of customers particularly those such as Money Transmitters where services are being provided on behalf of their own customers*
- *the costs of not meeting their obligations effectively- e.g. enforcement action, restrictions on activity and remediation work.*

6.1.1 Background on cost increases

Almost all the banks to which we have spoken have increased spending on AML/CFT compliance, including on-boarding, monitoring and second line functions. Most have increased compliance staff, and some have required the first line to own more of the process (resulting in shift of resource from the second line, but not a loss in overall compliance). Although a handful of smaller banks have not increased headcount, compliance time per client has still risen; they have typically avoided recruitment by reducing client numbers and/or allocating more general manager time. Several banks acknowledged that their resources in this area had previously been insufficient, and so there was a 'catch-up' taking place, both in terms of the increase in permanent staff and in remediation through reviews of existing clients. One branch of a foreign bank, for example, indicated that it had doubled permanent headcount, while the addition of temporary staff carrying out remediation had doubled it again.

In any event, compliance costs are bound to have increased since salaries for compliance professionals are up materially. One interviewee bank quoted £110k p.a. on a fully loaded basis (pensions, IT support etc.) for mid-ranking compliance professionals in central London. Compliance consultants are also charging significantly more (as are compliance staff head hunters). A Thompson Reuters survey[25] found that seventy-five percent of respondents in the UK and Europe expected the cost of senior compliance staff to increase in 2015.

Specifically, recruiter Robert Walters has recently disclosed its estimates of 2016 salaries for compliance professionals, including £175k for Money Laundering Reporting Officers £100k for central compliance, for regulatory affairs and for trade surveillance, £110k for monitoring/assurance and £220k for regional head of compliance. These figures may relate more to investment banks than retail/commercial banks, but ignore non-salary costs. They represent increases of 6% to 20% on 2015.

We would expect the market to adjust over time, but demand has increased so quickly that supply has not been able to keep pace. The resulting spike may get locked in due to the nature of contracts and recruitment. Clearly it would have been better, from a cost perspective, if there had been a more gradual increase in banks' perceptions of their compliance needs. There is also a concern over the ability of banks to hold out for the

[25] Cost of Compliance 2015, Thomson Reuters

most suitable staff given the keenness of many to grow headcount, or indeed about the total number of suitable staff who are available. Staff turnover is an accompanying issue both at banks and third party providers (and at the NCA's Financial Intelligence Unit).

A recent LexisNexis/ACAMS (Association of Certified Anti-Money Laundering Specialists) survey of global compliance professionals found that "*most organizations have increased their AML investment over the past three years – most by 10%-24%. Additionally, most organizations anticipate increasing their AML investment over the next three years – most by 10%-24%.*" The same survey identified a marked difference between large and small institutions – "the small financial institutions have invested little in their AML spend nor do they anticipate spending on AML activity in the coming three years, indicating that small institutions feel their compliance programs are able to meet the challenges of new regulatory expectations with minimal investment." This latter finding is not wholly borne out in our research in the UK and may reflect a bias in the LexisNexis/ACAMS survey towards North American based institutions.

6.1.2 Top-down data

Banks are generally reluctant to disclose figures relating to spending on compliance, but there are some data about global banks in the public domain. Although these have lesser evidentiary value and it is not always clear to which units of the banks they refer or indeed their accuracy, they are indicative of major increases[26]. Purely illustrative examples of such data include a quarterly rate of expenditure that has jumped from c.$130m to c.$240m in about two years; €1.3bn in extra regulatory-related spending; an extra 3,000 compliance staff employed in 2013; and the total number employed in compliance more than doubling to over 7,000.

Although these banks may be seen to be responding to extreme situations, including significant fines for AML/CFT shortcomings, the order of magnitude of cost and headcount changes is not unusual among our interviewees. A few examples are mentioned later in this section, and indeed one of the large UK banks (with data described in section 4) also provided some indicative cost figures for one team managing financial crime risk including higher risk customers. In 2012, this team had a budget of c.£100k while its annual cost run rate has now reached over £5m.

In the UK, the BBA estimates that its members are spending at least £5bn annually collectively on core financial crime compliance including enhanced systems and controls and recruitment of staff (not including the direct costs from fines for AML/CFT breaches). The BBA also understands that around 2,000 new UK AML roles were created in the banking industry in the past year.[27]

6.1.3 Limited granular data

Very few banks were able to provide figures for compliance costs on a per client basis, whether for onboarding or monitoring. A typical response is shown in Box 9 below. This is in part understandable since it may be difficult to distinguish the parts of these processes which are necessary from a non-compliance perspective (basic record-keeping, knowledge for future marketing, etc.). Further, compliance costs are split

[26] See, for just one example, 'Banks face pushback over surging compliance and regulatory costs' Financial Times, 28/5/2015

[27] BBA response to BIS Cutting Red Tape Review: The Effectiveness of the UK's AML Regime

across various teams, e.g. front-line, administration/record-keeping and financial crime. Nonetheless, we found it noteworthy that most banks are not using estimated compliance cost figures as an explicit input to the 'profit per customer' calculation. Anecdotally, we have heard this explicitly in the context of trade finance.

Interviews with smaller banks find that they have increased expenditure materially (50-100%). They may not increase further from here as they have been using consultants and temporary staff, a requirement which they hope will decrease.

In larger institutions, costs are inevitably split between various business lines and local and/or centralised compliance functions. In the cases at the larger banks where client-facing businesses are increasingly bearing more compliance costs, the frontline staff make their own judgements as to whether such costs are prohibitive. (The costs themselves are primarily determined by the compliance team who indicate required levels of due diligence and mitigation). We have not surveyed these employees to understand to what degree they take an explicitly quantitative approach, but such an approach may increase risk aversion (self-censorship).

Box 9: Bank response on costs

It is difficult to separate out specific compliance costs because in many instances a single process may satisfy more than one compliance / business requirement. A good example of this is the customer on-boarding process where a significant amount of customer data is collected, including, but not limited to:

- Customer / entity name;
- Relevant addresses;
- Purpose of account;
- Source of funds / wealth;
- Nature of business;
- Tax residency;
- Income / turnover;
- Business plan; and
- Occupation.

This information, captured at the outset of a relationship and refreshed throughout its duration, is essential to comply with various legislation and regulation (The Money Laundering Regulations. FATCA, Immigration Act, Sanctions etc.), it helps us to prevent and detect fraud and enables us to offer the right products and services to our customers based upon what we know about them. Because of this, it is not possible to attribute a specific cost of financial crime compliance to the account opening process.
Some processes such as the satisfaction of Court Orders or Transaction Monitoring are more discrete in nature, but it is still difficult to calculate the cost as it is not limited to the cost of the system deployed. Associated costs such as resource, training, system maintenance, property, IT equipment etc. should be considered as part of the overall cost. It is not possible to separate out the cost of monitoring higher risk relationships.

6.1.4 Example data

One bank has provided estimates of costs for due diligence for correspondent banking clients. Standard due diligence costs are estimated at c.£300 per client, however, all respondents undergo enhanced due diligence at £1,600-2,400, depending on the perceived level of risk. A further c. £400-500 per client is allocated for a dedicated financial crime team. So total on-boarding costs by the dedicated teams sums to around £2,300 for lower risk to £3,300 for higher risk.

Similarly, the same bank has estimated annual 'cost to serve' correspondent banking clients at £1,400 to £2,000, depending on risk level. This covers compliance-related monitoring costs (transaction checks, triggers, etc.) but also other non-compliance maintenance costs.

For enhanced due diligence, other than the rough figures for in-house checks for the large bank mentioned above, we have also been given a range of costs of £7-20k for external reports from a compliance/investigation consultant.

Box 10 provides a summary of some data provided by one bank covering a range of costs in the area of financial crime: screening, investigations, etc.

Box 10: Costs data from one bank

The data provided exclude the front line costs of the initial on-boarding, given the difficulty of separating these out from other front line costs. Rather, they focus on costs within teams related to screening and risk assessing customers and transactions, and to higher level policy-driven input (in this box all of these are collectively termed 'back office compliance costs').

The data are based on a single period (2015) rather than development over time.

Looking at the on-boarding of retail customers (including individuals and small businesses), dedicated teams (as opposed to front office) carry out sample checks on KYC data collection for a large proportion. These checks cost barely more than £1 per customer for individuals and £6 for businesses. Some of these customers of both types are referred for an additional screening, costing only about £1 each on average as most are rapidly discounted as they are false positives on name matches. A very small number, fewer than 0.2% of on-boarding retail customers, are referred for more detailed risk assessments costing £10-40 each, and a fraction of these are further escalated for senior expert oversight (c.£110 per customer).

The process is analogous for corporate customers, but the on-boarding checks costs around £40 per client, the automated screen c.£2, and the detailed risk assessment c. £160, for around 1% of new corporates. Senior oversight for a fraction of these costs c. £220 each.

Some customers require FATCA reviews, costing a further c.£4 each, and a small number (not provided) are referred to the FIU (c.£34 each).

Box 10: Costs data from one bank cont.

Some clients are referred to another, higher level financial crime compliance team (which is also responsible for policy, training, assurance, governance and reporting). The bank has not attempted to allocate these on a per customer basis, but some of these referrals can result in a process lasting months, specifically if a referred client is a sanctioned individual/entity.

New to bank customers appear to account for around 20-25% of total back office compliance crime costs. The same teams are responsible for on-going monitoring, accounting for the balance of costs. The bulk of monitoring costs relate to reviews of existing customers, primarily periodic, transaction screening, which may itself result in customer reviews, and suspicious activity triggers.

12-14% of existing retail customers and c.67% of corporates are reviewed each year. The basic screening costs £1-2 per retail or corporate customer. 2-3% of these undergo a more detailed risk assessment (£35 each for retail and £160 for corporates). Of these, c.20% are escalated for senior expert oversight (c.£110 for retail and c.£220 for corporates).

An undisclosed proportion of payments are screened at a cost of c. £0.5 each. C.0.3% of these are escalated for further investigation, costing c.£26 each.

Separately, a small number of transactions directly trigger a suspicious activity report, which is investigated at a cost of c.£42 each.

Please note that at least a quarter of back office compliance costs, and all compliance costs relating to the front office, are not included in the 'per customer' figures above, so all are understated.

Looking at the overall back office compliance costs, as mentioned above around 20-25% relate to on-boarding, around one half relate to reviews of the existing customer base and the balance to payments screening and suspicious activity triggers. These figures equate to perhaps 70-80p per retail client p.a. and £15-20 per corporate client.

6.1.5 Headcount as a proxy

Other than this, on a bottom-up basis we have asked banks for today's headcount and the change over time. We are generally finding staff numbers have increased by 30-100%, which would imply a cost increase well above these figures. In one of the more extreme examples (a branch of a foreign bank), compliance staff numbers have quadrupled – an easier thing to achieve from a low base rate - but half of these staff are temporary and, according to the manager, relate to the bank playing catch-up after having spent insufficiently over the previous decade. One could consider some of this expenditure as remediation, even without actual censure from a regulator.

In another foreign bank example, headcount tripled, and with a parallel fall in customers this resulted in our estimate of annual compliance cost per customer, on a broad definition, rising from £60-70 to c. £300.

6.1.6 Impact on profitability and debanking

Coupled with higher capital requirements and reduced deposit margins, the increase in compliance costs must have changed the profitability per client calculation across the board. Inherently, this will move certain clients, especially those which generate disproportionately high levels of capital and compliance resources, the wrong side of the bank's profitability target. We think this can explain many of the closures of active client accounts. We find it interesting, however, that most banks are not articulating this change in an explicit way, or supporting their actions using example figures. This suggests that many such decisions are made on a more qualitative basis, with a gut feel of costs and profitability. A simplification of this qualitative process might be that a *prima facie* policy line reduces costs of intensive case-by-case examination, just as it does in regulation.

As discussed elsewhere, there will also be account closures of profitable accounts where banks consider that, no matter how much they spend on due diligence and mitigation, they are not able to sufficiently reduce to an acceptable level the risk of an outsized fine/sanction, and indeed of the potentially even more damaging reputational impacts. Examples might include MSB third party payments, pay-through accounts, where they have no visibility on the underlying business and where they have no confidence that media and regulators will take other than a zero risk appetite.

6.1.7 Mitigating compliance costs

We found little appetite to share increased compliance costs for bank accounts with customers on the basis of their ML/TF risk rating, either collectively or (especially) individually, even if such costs could be calculated. Some of our interviewees thought this might be seen almost as a "bribe" to keep undesirable business; concerns were also expressed that this would reveal risk ratings to customers, which would be bad practice and lead them to 'game' the system. Without specific examples, we were told by some that they feared the FCA would frown on such differential pricing as an example of not treating customers equitably, although it would represent a concrete example of the RBA.

Our own view is that some banks are being too cautious here, and a clearly articulated policy of passing on higher compliance costs to clients would be recognised as good practice by regulators and professionals, just as banks pass on higher funding costs, for example, Some clients might complain, though others would realise that this was superior to losing their account altogether. Some might seek cheaper banking elsewhere. The risk we have identified is media risk ('reputation' might be a bit strong a term), i.e. "I've been with xx bank for 10 years and now they've suddenly increased my annual fee tenfold".

A small challenger bank, starting its customer base with a clean sheet, indicated to us that it had not even considered charging higher fees to certain clients for compliance reasons, and planned to ration 'high risk' clients based on in-house compliance capacity.

6.2 For Customers

FCA questions:

- *how much does a higher risk customer such as a money transmitter pay for a business account? How are those costs charged to the customer in terms of upfront costs; monthly/annual costs, other costs (e.g. additional compliance measures required by a bank)?*
- *a comparison to a 'standard' risk customer*

As above, we have been told that *differential* pricing is not charged for retail/SME account facilities on the basis of judged ML/TF risk. It is a frequent response from those who are under threat of derisking to offer to share the costs incurred, but as we have seen above, either (a) banks would be unwilling to enter into such arrangements and do not have good data on the cost of enhanced AML/CFT controls for specific customers or (b) charging more (in order to deploy enhanced control measures) is not a sufficient mitigation to the perceived risk. Revenue generated from particular accounts may be important, but banks are reluctant to state specifics. It has been characterised to us that the banks' business lines will have a 'general feel' for both profitability and costs.

One more charitable way of looking at the limited calculation (and passing on) of customer-specific compliance costs is that it is a type of insurance policy in which premiums are based on largely estimated/guessed data rather than real claims, i.e. that the costs of actual sanction events or reputational hits are ultimately more important to the bottom line than the cost of day-to-day compliance.

7 MITIGATION OF DERISKING PROGRAMMES

FCA question: Various bodies are doing work domestically in the UK and at an international level through various bodies such as FATF and the World Bank on derisking. The supplier will be expected to establish through its fieldwork whether this work has had any impact on banks' risk appetites.

As discussed in Section 3, we assess that mitigation attempts using public statements by FATF, FCA and US regulators are somewhat missing the mark, by focusing on 'wholesale v case-by-case' derisking. The banks we have spoken to either do not believe they are derisking in any of the senses of the word in this context, or believe that they are carrying out risk-based management of their higher risk clients in a way that could be described as case-by-case derisking. Some of our interviewees were not in favour of the terminology 'derisking' in any case, believing it has become pejorative. Others use derisking to describe the results of their RBA generally, not specifically exiting or refusing accounts.

Generally, banks have told us that they are seeking much more specific guidance on managing high-risk relationships of the types that have led to account exit or refusal if there is a criticism from regulators and government that they are behaving improperly. Some compliance officers seek a full legal safe-harbour; some, perhaps more realistically, ask for more particulars on what are deemed by regulators as acceptable levels of risk.

One large global bank indicated that it would prefer prescriptive regulation (and stability of regulators and regulations), giving certain Asian regulators as examples (though it also acknowledged cultural differences). The revised JMLSG guidance relating to MSBs is regarded as helpful by some, whilst others believe it adds nothing to their current practices and it certainly falls well short of a safe harbour, despite some (predominantly US) literature suggesting it provides one[28].

We received comments on some specific issues raised in mitigation. The question of 'knowing your customers' customer', where both FATF and supervisors have clarified that financial institutions generally have no obligation to carry out due diligence on underlying customers is one such. For example, according to the FATF in June 2015[29], *"Although there will be exceptions in high risk scenarios, the FATF Recommendations do not require banks to perform, as a matter of course, normal customer due diligence on the customers of their respondent banks when establishing and maintaining correspondent banking relationships."* Banks tell us that they fully understand that explanation and have no intention of carrying out such due diligence as a matter of course, but in higher risk circumstances (and beyond correspondent banking) they feel they must know something about the underlying customers, for example when they are processing payments, which may involve sanctioned countries or entities.

If they do not have sufficient confidence in the AML/CFT controls implemented by their customer (e.g. another bank or payment institution) they believe they must

[28] This report was finalised before the FATF published its own revised *Guidance for a Risk-Based Approach for Money or Value Transfer Services* in February 2016 - http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-money-or-value-transfer.html

[29] *Drivers for "de-risking" go beyond anti-money laundering / terrorist financing,* FATF, June 2015 - http://www.fatf-gafi.org/publications/fatfrecommendations/documents/derisking-goes-beyond-amlcft.html

mitigate the underlying risk themselves. There is a widely held belief that if they were caught up in a payment chain involving financial crime or sanctions breaches, they would have legal liability for that breach, even if they did not have an obligation to know the underlying customer.

The well-documented fines for egregious AML/CFT breaches have clearly led to a more risk averse attitude to ML/TF risks. Attempts have been made by regulators to mitigate bankers' fears by pointing out that these fines have not been levied for simply banking MSBs or for failure in controls in a bank's customer, but rather for serious failures in controls in the banks themselves. However, there is no evidence that this reassurance has had any particular effect (including no effect) on derisking behaviour. In fact, there is a perception within banking, however undeserved, of a 'zero tolerance' to all ML/TF risks by supervisors.

Indeed, given bankers' perception that the global jurisdiction claimed by the US regulators and courts can place their conduct *anywhere* under sanction, it is not clear what reliance should rationally be placed on such reassurances from their local supervisors by non-US institutions who rely on access to the US markets, even though US Federal authorities have joined in the reassurance, and might be expected to apply this to their own decisions on penalties.

The fines appear to have had their (presumed) desired impact of focusing minds at all levels (first and second line, senior and executive management) on the risks that ML/TF pose to the institution and its reputation, which has almost inevitably led to a more risk-averse attitude, irrespective of the exact nature of the breaches. This may change as banks work through their various strategic, commercial, remediation and AML/CFT review programmes, but for the time being we anticipate that banks will continue to retrench to their core business and continue to exit certain customers for a variety of reasons.

8 METHODOLOGY

The method used to compile this report was as follows.

Literature overview

We reviewed a wide range of research, regulatory guidance and statements, opinion and campaigning pieces and general press coverage to identify original evidence relating to derisking by UK banks that was not widely known (known unknowns) and sources that might yield such evidence (unknown unknowns). We also attended or reviewed several webinars. It became apparent that more UK-focused evidence would be obtained by focussing on prime sources than on literature, which is often general and anecdotal in nature. Pointers to sectors affected were found in the literature, as was a limited amount of data, which were used to inform our research or is included in the report where appropriate. Thus no separate literature review section has been included.

Collection of data from banks

We conducted discussions with subject experts and used these to identify the types of data that banks were likely to have in order to operate profitably and sustainably, both as individual institutions and at association level. Based on these general data types, we developed a set of high level questions to put to banks, and a list of specific performance data which might provide quantitative and qualitative evidence of derisking and its drivers and impacts. We derived a complementary set of general and specific data requests at association level.

We endeavoured to reach banks, to conduct written or spoken questionnaires, in four ways: following the FCA's roundtable introductions (UK clearers and large international banks); AFB introductions (foreign banks with small/medium UK subsidiaries and branches); BBA introductions; our own contacts. Unfortunately, we were unable to gain as much access to banks via the BBA route as hoped, leaving us with fewer UK small and medium-sized bank contacts than expected, although we did attend a BBA Anti-Money Laundering Forum session and gathered views in a roundtable format.

We spoke with 24 banks in one-on-ones and had indirect, data gathering contacts with 15 more (also via bilateral communications). Additionally, we communicated with a further 20-25 banks via roundtable discussions. The FCA asked us to especially target the big 5 UK banks, and we asked these banks a larger set of questions than most others. For others we focused on the primary questions, tailored to match the business mix of the institution and the individual(s) to whom we had access.

We also spoke with single sector and umbrella associations representing various industry and community sectors with whom we discussed the general questions and explained the relevance of the specific data requirements.

Collection of data on those derisked or at risk of derisking

The issue of derisking in relation to MTOs is well known, and substantial amount of data on it already exists, so we focussed on sectors where data was less known or available.

On the basis of literature review, talks with experts and first principles, we identified a number of areas where we thought there may be problems, to which were added areas where the FCA has received representations from those claiming to face, or those who have already experienced, derisking. Among these were a number of associations via whom we gained access to grass roots members.

We also engaged with government departments with knowledge of derisking, and used semi structured interviews to establish any evidence of derisking in the areas under their purview. In particular, we held discussions with the Gambling Commission, Charities Commission and HMRC.

Evaluation of Data

We collected accounts of derisking and the triggers for derisking as perceived by respondents, from which we built up a general pattern of derisking. However, the number involved being small (units and low tens) it was not possible to undertake any statistically significant numerical analysis. We did identify areas where there appeared to be a significant incidence of derisking, and areas where there was no evidence of the derisking that was commonly believed to exist (but the absence of evidence does not equal the evidence of absence).

Treatment of specific issues

- Drivers of derisking: By requesting detailed information on the policies and procedures leading to account closure/opening decisions, discussions with, and information requests to, banks we were able to explore the risk and economic factors at play and assess their role and significance in bank closure decisions. We also discussed with banks the impacts of the mitigations of derisking.
- Exclusion costs of derisking: These impacts included, for non-banks, difficulty and delay in accessing accounts, having to find alternative arrangements as a result of account closure and costs of specialist services or financial exclusion. They were mainly obtained by question and answer among 'victims'. For banks, discussions covered impacts on the (small/medium) banks of actions and communications by larger banks (correspondents, agents, clearers etc.). They also included, on occasion, the impact on the banks' clients, some of whom they felt they could no longer service. Finally, the impacts of derisking by larger banks were blended with the responses of the small/medium banks to the perceived changes in the regulatory environment, including an increase in the cost of their compliance and financial crime units.
- The costs of on-boarding, monitoring etc: our efforts here concentrated on the banks we were surveying, of all sizes. Since, as anticipated, none were able initially to provide clear answers to such questions as how much does it cost to on-board or monitor a customer, we worked closely with some banks to help them come up with estimates, and for some endeavoured to understand aggregate costs, at least for 'back office' functions, by comparison with the number of customers. We also asked how such costs had changed over time.
- NGOs: We held a round table with a cross section of charities and made follow up calls.
- Diplomats/PEPs/Crown/Civil Servants: We contacted the government official dealing with this for the FCO.