BLP Corporate Crime & Investigations column: April 2017

by by Robin Ganguly, Joanna Harris and Alexandra Hildyard, ***Berwin Leighton Paisner LLP***

Articles | Published on 24-Apr-2017 | England, Wales

Berwin Leighton Paisner LLP's Corporate Crime & Investigations team is led by Aaron Stephens. The team regularly share their views on topical corporate crime and investigations issues with our subscribers.

Appeal decision in N v S

In *N v S [2015] EWHC 3248 (Comm)*, Burton J disapplied the Proceeds of Crime Act 2002 (POCA) consent regime for dealing with funds that may be the proceeds of crime (BLP acted for the bank (S) in the first instance) (see *Article, BLP Corporate Crime & Investigations column: April 2016*). The National Crime Agency (NCA) appealed and the Court of Appeal handed down its judgment on 7 April 2017 (*National Crime Agency v N [2017] EWCA Civ 253*; see *Legal update, A court cannot make orders for interim relief that dis-apply consent regime under Proceeds of Crime Act 2002 (Court of Appeal)*).

At first instance, Burton J was faced with an urgent application for an injunction by the bank's customer (N) to compel the bank to carry out transactions on the customer's accounts (the accounts were frozen following the bank's report to the NCA that it suspected that they contained the proceeds of investment fraud). Burton J granted the injunction and gave an accompanying declaration that in operating the accounts the bank would not commit a criminal offence under POCA or otherwise. This effectively ousted the POCA consent regime. Accordingly, it was a departure from previous authorities, in which the courts determined that the POCA regime should not be interfered with, on the basis that it had been enacted by Parliament to provide a workable balance between the rights of private parties and the need to prevent money laundering. The NCA appeared as an interested party before Burton J and subsequently appealed his decision.

The Court of Appeal allowed the NCA's appeal. On the issue of whether the court has jurisdiction to override the POCA consent regime, the Court of Appeal found that ordinarily the court should not intervene within the POCA seven-day notice and 31-day moratorium periods, but noted that the court does have jurisdiction to grant interim relief in appropriate cases (albeit that the statutory procedure should be highly relevant to the court's determination of whether to exercise its discretion to do so, and will usually be determinative). The Court of Appeal found that the customer's potential losses did not constitute sufficient justification to displace the statutory regime. Regarding the interim declaration of no criminal liability (which fed into Burton J's analysis of the balance of convenience), the Court of Appeal found that such a declaration should only be given when the court has a high degree of assurance as to the recipient's entitlement to such a declaration. In this case, where there was no detailed exploration of the bank's suspicions and likelihood that the accounts actually contained criminal property, the court did not have that assurance.

The first instance decision had potentially opened the floodgates for bank customers to seek injunctive relief to unlock frozen accounts. However, the appeal decision re-confirms that a court's assistance cannot easily be obtained in these situations. The Court of Appeal's finding that *N v S* (in which the bank's customer was a payment services provider and feared the collapse of its business as a result of the freeze) was not a case in which court intervention was justified poses the question of exactly what would be required in order to depart from the statutory procedure.

Deutsche Bank FCA final notice: key takeaways for firms

On 31 January 2017, Deutsche Bank AG (DB) was fined £163 million by the *Financial Conduct Authority* (FCA) for failings in its AML control framework, in addition to being fined USD425 million by the New York Department of Financial Services (DFS) on 30 January 2017 (see *Legal update, FCA fines Deutsche Bank for serious AML control failings*).

Both the FCA final notice and the DFS consent order serve as a reminder of the cost of failing to comply with relevant regulatory requirements. They are also valuable resources for firms seeking to understand regulatory expectations around AML compliance. Indeed, the FCA final notice states that an aggravating factor in determining DB's fine was that, given past enforcement action taken by the FCA in respect of similar failings by other firms as well as relevant guidance - the bank should have been aware of the importance of appropriately assessing, managing and monitoring the money laundering risk associated with its corporate banking and securities division in the UK.

What happened?

As a result of the deficiencies in DB's AML control framework, between 2011 and October 2014 thousands of "mirror trades" were used by connected customers of DB and DB Moscow Ltd to transfer more than USD10 billion from Russia, through DB in the UK, to overseas bank accounts without detection.

The FCA fine was based on breaches of PRIN 3 and the SYSC rules on AML controls. While it was not proven that DB's customers (or their underlying clients) were laundering the proceeds of crime, the way the trades were conducted, in addition to their scale and volume, was deemed to be "highly suggestive" of financial crime.

In particular, between April 2012 and October 2014, 2,400 mirror trades involved the following arrangement:

- A Russian customer of DB Moscow bought liquid Russian securities (that is, shares in well-known, listed entities) from DB Moscow and paid in roubles (the "Moscow Side").
- A non-Russian customer of DB London (who had been on-boarded by DB Moscow) sold the same securities to DB London for US dollars. Sometimes these trades would be booked on the same day (the "London Side").
- The London Side trades were remotely booked by DB Moscow.

In addition, "one-sided trades" were also identified between January 2012 and February 2015. The FCA takes the view that some, if not all, of these trades must have formed one side of an additional 3,400 mirror trades.

Hallmarks of the trades included customers trading on behalf of underlying clients, and entities being connected to each other, usually by common ownership. There was also a lack of commercial rationale for the trades and the customers in fact usually lost money in fees.

Key takeaway points for firms

Ensure clear allocation of responsibilities for AML compliance and that the front office is aware of its vital role

The FCA found that the London front office failed to appreciate that it was ultimately responsible for the know your customer (KYC) obligations of its customers, even if the customers were on-boarded by the Moscow office, and instead regarded the customer on-boarding team (COB team), based in India, as being responsible. However, the FCA found that the COB team was only there to perform a process-driven administrative function of checking documents.

In this context, the Moscow office was able to on-board customers to the London office for use in the London Side trades without applying the same standards as the London office, and the FCA found that this contributed to the "poor quality" of the information on file for the mirror trading customers. In particular, the following deficiencies were found:

- Lack of evidence regarding source of wealth and funds.
- Lack of information regarding the purpose of the business relationship.
- Failure to independently verify the ownership structure provided by the customer.
- Failure to identify ultimate beneficial owners (UBOs) and to highlight that customers shared the same UBO or representative. After being on-boarded, the relationship with the relevant customers was also managed by Moscow front office.

It is therefore clear that if any overseas group company or branch is capable of on-boarding customers for a UK entity, this process must be carefully managed and supervised by all three lines of defence in the UK entity, and the same standards must be applied. In particular, collecting sufficient information around source of funds or wealth and purpose of business relationship should be a key focus.

Only rely on the CDD of another firm in the circumstances permitted by the Money Laundering Regulations and JMLSG guidance

The FCA found that DB failed to ensure that customer due diligence (CDD) was conducted on the underlying clients of DB's customers (who were acting as intermediaries). One reason for this was that DB's AML policies indicated that, for a regulated customer, reliance could be placed on the presumed CDD conducted by the customer. However, in doing so the policy failed to note an important caveat: namely, if a relevant person establishes a business relationship with, or conducts an occasional transaction for, the underlying client of another business (such as an intermediary), the relevant person may rely on the CDD measures of the other business in certain circumstances. However, if the other business operates in a non-EEA jurisdiction, reliance is only permitted if the other business is subject to both mandatory professional registration and to AML requirements equivalent to those promulgated by EU money laundering directives. Russia does not fulfil these requirements, and therefore DB should not have placed reliance on the presumed CDD of its Russian customers.

This issue also serves as a reminder of the importance of undertaking a "gap analysis" of existing policies and new policies before they are introduced.

Check and double check your policies

The FCA found that there were various deficiencies in DB's policies and procedures. These included not requiring the London front office to supervise the on-boarding of clients by the Moscow office (see above), as well as a lack of guidance on how to establish the legitimacy of a customer's sources of wealth or funds or a requirement to gather information about expected account activity.

Further, when identifying and verifying a customer's UBOs, the AML policies only focused on those individuals who owned or controlled 25% or more of the shares of a business. However, under Chapter 3 of the Financial Crime Guide, it is poor practice not to consider all those individuals who exercise de facto control over the management of a corporate customer, regardless of shareholding.

Get your risk ratings right ... or everything will go wrong

The final notice identified particular issues with the bank's risk rating methodology. This led to mirror trading customers being miscategorised as medium or low risk when many were, in fact, high risk. As the AML team only routinely reviewed high risk clients, the customers in question were not subject to review by the AML team during the on-boarding process. Indeed, the FCA found that during the relevant period, only 5% of DB's customers were categorised as high risk.

The risk rating given to a customer is the basis from which all monitoring requirements flow. This means that getting it right is vital. Risk ratings should be monitored or spot-checked to ensure standards are being maintained and policies and procedures are not being circumvented. It is also worth looking at the percentage of customers that are marked as high risk overall and ensuring that this is maintained at the expected level.

Make sure your IT systems are speaking to each other

DB lacked a single authoritative repository of KYC information because it used multiple IT systems. One significant consequence was a lack of reconciliation between the trading and customer on-boarding systems. As a result, the bank was unable to connect trading activity with underlying KYC information.

The DFS also noted that the lack of a central repository meant that when one trading counterparty was suspended, a related trading counterparty could be re-on boarded without raising any red flags.

Transaction and payment monitoring

DB's global AML policy required the implementation of systems to monitor customer accounts for unusual or suspicious transactions. However, the bank did not implement any divisional policies or key operating procedures in the UK for transaction monitoring or the escalation of suspicious activity to the AML team.

Further, the London front office considered DB Moscow to be responsible for monitoring the remotely booked trades. However, this was misplaced as Moscow's trade monitoring team did not actually have access to data about those trades.

Fully resource your compliance department

The FCA noted that a lack of resources hampered DB compliance, contributed to problems and meant that red flags and warning signs were not followed up. The message: make sure compliance has sufficient resources.

Other developments on the Anti-money laundering front

March 2017 was a busy month on the AML front. Below we report on various developments.

Consultation on the transposition of the Fourth Money Laundering Directive

The Fourth Money Laundering Directive (*(EU) 2015/849*) (4MLD) aims to give effect to the updated Financial Action Task Force Standards by introducing new requirements on financial services businesses and changing some of their existing obligations under the Third Money Laundering Directive (*2005/60/EC*).

The deadline for the UK to transpose 4MLD into UK law is fast approaching and the government's evidence gathering process is coming to a head. On 15 March 2017 the government published its response to its consultation *Transposition of the Fourth Money Laundering Directive* and with it the draft Money Laundering, Terrorist Financing and Transfer of Funds (Information of the Payer) Regulations 2017 (MLR 2017). The response includes the government's policy positions in the light of the 186 responses it received to the consultation and a call for further information. Responses to the government's call for further information are due by 12 April 2017, after which the government must finalise the MLR 2017 ready to come into force by 26 June 2017.

A striking feature of the UK government's approach is its emphasis on sector-specific risk assessments and guidance. The government recognises that "too much prescription in legislation may lead to a 'tick-box' approach" and that firms and supervisors are best placed to understand their individual and sector risk profiles. Through the new legislation, the government therefore obliges and encourages firms to assess risk and apply proportionate and bespoke controls. In the context of ongoing monitoring of existing customers (and to assist in this undertaking) a summary of risk factors from 4MLD is included in the MLR 2017. In addition, the government is consulting specifically on the quality and consistency of supervision and guidance across different sectors.

Other changes to be introduced by the MLR 2017 include:

- Replacing the existing list of products that may be suitable for simplified customer due diligence (SCDD) with a non-exhaustive list of factors, to be supplemented by sector-specific guidance (see further below).
- Expansion of the types of third parties that can be relied on to meet a firm's CDD requirements.
- Clarifying that lettings agents will continue to be within the scope of the MLR 2017 to the extent that they carry out "estate agency work" as defined by the Estate Agents Act 1979, but stopping short of extending the regulations to cover lettings activity itself.
- Clarifying that for the purpose of the regulations, an estate agent shall be considered to be entering into a business relationship with both the purchaser and the seller (and shall be obliged to carry out CDD on both parties).
- Expanding the definition of politically exposed person (PEP) to include UK PEPs along with their family members and known close associates, and introducing a more flexible and differentiated approach to PEPs generally (note that the consultation states that the government would expect that UK PEPs should generally be regarded as lower risk). For more information on the FCA draft guidance on the treatment of PEPs, see *FCA guidance on the treatment of domestic and foreign politically exposed persons (PEPs)* below.

For more information on the MLR 2017 and the consultation, see *Legal update, Draft Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 published*.

Cutting red tape and consultation response: AML supervisory regime

The government's *Call for Information on the UK's AML Supervisory Regime* dovetails with its *Cutting red tape review of the UK's AML and counter financing of terrorism regime*. The Cutting Red Tape review aims to identify and remove unnecessary regulatory burdens on firms while strengthening and improving the efficiency of the AML and counter terrorist financing (CTF) regime. This means identification and streamlining of repetitious (or worse, contradictory) guidance and supervision across sectors to assist firms and supervisors in developing and guiding on a proportionate and risk-based approach to the AML and CTF regime. Hence the government elected to publish a combined response to both the Cutting Red Tape Review and the call for evidence on the supervisory regime on 16 March 2017.

The most significant development that comes out of the response document is the government's intention to introduce a new Office for Professional Body AML Supervision (OPBAS) to work with professional supervisors to ensure consistency of approach across the sector.

This proposal is geared to address concerns that supervision by the 23 active supervisors which operate across various sectors is inconsistent and of varying quality. In particular, respondents identified a need for the government

to set "clear standards for effective supervision with detailed guidance and greater oversight to help supervisors comply effectively."

Importantly, respondents took the view that it was oversight that was required and not replacement of existing supervisors with any single body. Respondents consider there is a strong advantage in having a range of AML supervisors with sector-specific experience, as this "ensures that a diverse range of innovative products are fully understood and that their risks are minimised."

OPBAS will sit within the FCA and will be positioned above (rather than replacing) the existing supervisory regime. It is hoped that this will maintain a diversity of expertise while improving consistency of approach. However, there is a risk that creation of another supervisory body will only add to the heavy regulatory burden already facing firms and the precise scope of OPBAS's role and the powers it will have remain unclear. The government intends to consult on draft regulations to underpin OPBAS over the summer and expects the office to be fully operational by 2018.

Guidance from supervisors, the JMLSG and FCA

A further area in which respondents identified a need for consistency and streamlining is guidance. Both the respondents and the government acknowledge this is no simple undertaking as there is great value in the sector-specific guidance produced by different supervisors but equally the need for consistency of approach.

The guidance issued by the FCA and joint money laundering steering group (JMLSG) are both acknowledged as being extremely valuable. However, it is recognised that they are not as streamlined and complementary of each other or of the supervisors' specialised guidance as they might be.

To improve consistency across all guidance and yet ensure that guidance continues to be tailored to the nature and risks of each sector, the government proposes:

- That new streamlined guidance be produced by each supervisory body with oversight from the Treasury.
- That the JMSLG and FCA guidance be updated in the light of the MLR 2017 and reviewed by the Treasury to ensure that they clearly complement each other and the single sector guidance.

To that end, on 21 March 2017, the JMSLG published proposed revisions to Part I of its guidance on the prevention of money laundering and the financing of terrorism for the UK financial services industry. This guidance will be subject to input from the Treasury before it is finalised. (See *Legal update, JMLSG proposes revisions to Part I of its guidance* and *Practice note, JMLSG AML and CTF guidance for the financial services sector*.)

FCA guidance on the treatment of domestic and foreign politically exposed persons (PEPs)

MLD4 broadens the definition of PEP to a person holding a politically exposed position in the UK (previously the definition was limited to PEPs from non-UK jurisdictions). To prevent this expansion of scope placing an undue burden on firms, on 16 March 2017 the FCA published updated, draft guidance to assist firms to evaluate risks posed by various types of PEPs and apply proportionate controls. Publication of this guidance is a requirement on the FCA (*section 333U, Financial Services and Markets Act 2000*).

The guidance provides a (non-exhaustive) list of geographic and personal and professional factors that may assist firms to evaluate the risks posed by different types of PEPs. Personal factors that indicate a PEP may pose a low risk include being subject to rigorous disclosure requirements and where an individual has not held a prominent public function for at least 12 months.

Geographic factors that the guidance specifically identifies as indicating that a PEP poses a low risk include solely operating in a country that has low levels of corruption along with political stability and free, fair elections. Significantly, the UK is singled out as one such country. This indicates that, although the definition of PEPs now covers UK PEPs, the FCA considers it will be rare that the most stringent due diligence procedures will be appropriate for such persons.

At the other end of the spectrum, personal and professional factors which may indicate a PEP poses a high risk include allegations of misconduct and finances derived from not obviously legitimate sources. Geographic factors include non-democratic forms of government and weak AML defences.

The guidance also includes non-exhaustive recommendations by the FCA of measures to take in both high and low risk situations. The measures proposed in high risk circumstances are comprehensive and resource intensive, including taking intrusive and exhaustive steps to establish the source of wealth or funds and regular formal reviews of the business relationship to establish whether or not it should continue. However, interestingly the FCA makes it very clear that "there should be relatively few cases where it is necessary to decline business relationships solely because of anti-money laundering requirements and, in relation to this guidance, this should only happen where PEPs pose a high money laundering risk". This is aimed at the issue of "de-risking", and seeks to ensure that firms take a proportionate approach to their obligations under the regulations and do not wrongfully exclude PEPs or close family or known associates from the banking system where further consideration would have identified that there was no cause to do so.

END OF DOCUMENT

