Money Laundering Bulletin, October 2009, Issue 167

***Mark Dunn**, Market Planning Manager, Risk & Compliance, LexisNexis*

PEP Check

Firms continue to struggle with their obligations around politically exposed persons (PEPs) – how far does and should the definition extend? How can they be identified? What about customers who only become PEPs after take-on? How frequent and detailed ongoing monitoring is enough? Mark Dunn of LexisNexis examines both the issues and practice.

Few anti-money laundering (AML) practitioners need reminding of the requirement under the Money Laundering Regulations 2007 (MLR 2007) to determine whether their customer is a politically exposed person (PEP). The enactment of the Regulations in December 2007, building on the earlier FATF Recommendation 6 and subsequent changes to the Joint Money Laundering Steering Group (JMLSG) Guidance, brought PEP checks to the regulated masses for the first time.

To briefly recap, according to a firm's risk-based approach a regulated entity must determine whether their customer is a PEP and screen family and other close associates as appropriate. Having determined if their customer is a PEP, management approval must be given before establishing a business relationship. In addition, the source of wealth and funds involved should be established and where the business relationship proceeds, enhanced ongoing monitoring of this relationship must be conducted. The need to conduct PEP checks and treat these business relationships as a higher risk is a direct result of the fallout experienced by banks and other institutions in the past where millions of dollars of wealth acquired by political figures like Sani Abacha (late president of Nigeria) and Ferdinand Marcos (late president of the Philippines) have been linked to corruption and money laundering, leading, ultimately, to increased enforcement, significant business losses and damaged corporate reputations.

The ability to apply a risk-based approach has inevitably led to organisations interpreting this requirement in different ways depending on each firm's perceived exposure to PEPs and the nature of the business conducted with these individuals and their associates. Many of the larger global financial institutions with the most to lose have bundled PEP checks in with similar checks against sanctions and law enforcement watch lists. In some cases, companies are deploying sophisticated transaction monitoring services, ID verification systems or other customer due diligence (CDD) tools to check individual clients en masse in batches of hundreds of thousands or even millions of names at a time. The content driving these services comes from established players like Dow Jones Risk & Compliance, World-Check and others, who employ teams of researchers to maintain lists of PEPs, their accompanying biographies and any identified links to high profile associates.

Many institutions will also go beyond the regulatory call of duty and will apply a broad brush approach to PEPs regardless of the definitions set out in the MLR 2007. Even where a PEP may hold a prominent public function in the UK or where they may be a former PEP who has not been active within the "preceding year" as outlined in the Regulations, firms may still treat these individuals with the same level of risk as a new PEP who has just arrived offshore with a suitcase full of money. In many cases, the adopted policy is "Once a PEP, always a PEP" regardless of jurisdiction and current occupation to ensure as little exposure to risk as possible.

Outside of the bigger institutions, companies may simply run ad hoc checks against a limited PEP list on a single name at a time as appropriate. This approach is in line with a need to screen lower volumes of new clients and a reduced exposure to high risk jurisdictions and cash rich transactions. Some firms may negate technology altogether and instead rely on their relationship managers and fee earners simply asking clients – "Are you a PEP? – Yes or No" and ticking a box on the CDD form.

The ambiguity surrounding the application of a 'risk based approach' to anti-money laundering not only impacts the extent to which firms tackle the initial screening of PEPs but also how they comply with the requirement to apply "enhanced ongoing monitoring" of these business relationships. Firms obviously rely on their relationship managers and fee earners to maintain an effective dialogue with their clients and be alerted to any significant changes in their circumstances. However, as before, where the risk is perceived as highest, technology is also deployed to continuously monitor those customers identified as PEPs against the latest editions of sanctions and watch lists to ensure that none of these individuals in the customer base suddenly appears on a blacklist without the firm knowing about it, thus enabling Compliance to rapidly respond as necessary.

However, the risks associated with PEPs rarely diminish as, by their very nature, prominent public figures unfortunately continue to be magnets for scandal, allegations of misconduct and more serious criminal investigations. Incoming regulations also put greater scrutiny on dealing with officials both in the UK and abroad. Proposed measures within the UK Bribery Bill prompt firms to review their anti-bribery and corruption policies and procedures to ensure their customer-facing staff and any intermediaries employed by the firm are aware of the risks, not only of blatantly making bribes but, more importantly, being perceived as inadvertently suggesting a bribe or similar inducement.
As a further example, the *Counter Terrorism Act 2008* Schedule 7 and its proposed 'directions' also bring high risk jurisdictions, and by association the PEPs residing in these countries, under further scrutiny with the need to quickly react to new sanctions and business cessation measures likely to become a reality.

This perennial backdrop of PEP risk, heightened regulatory scrutiny and other wider issues across the enterprise highlighted by the economic downturn (eg, supply chain exposure) has led firms to look for new ways to conduct enhanced ongoing monitoring. Borrowing from principles first established by PR agencies, technology is now being deployed to monitor high risk relationships against not only traditional sanctions and watch lists but also more general media and user generated web content. This technology enables firms to be alerted to those early indicators of negative sentiment that may signal an emerging issue that in turn could quickly escalate into a significant business risk. Although this approach sounds extreme, when millions of dollars are at stake and hard earned reputations are on the line, the earlier the warning of trouble ahead, the greater the time to react and mitigate the likely impact. As an example, recent events regarding the Allen Stanford case demonstrate the power of such technology. On this occasion, Alex Dalmady, a financial analyst, had reviewed Stanford's company accounts for a friend who was interested in conducting some business with the firm. The analyst found some issues in the company's report, wrote an article describing these findings, which was then published by a niche web source. This article was subsequently picked up and blogged across the world raising the negative sentiment on Stanford weeks before his subsequent arrest for alleged fraud.

One area of contention is how to deal with existing customers, who, in the course of the business relationship, become PEPs by appointment or through marriage. This is a very difficult area to police given that anyone in that part of the customer base deemed a low risk at the account opening stage could in theory assume the higher risk status of a PEP at some time in the future. Again, it's really down to the risk-based approach that each firm chooses to adopt, applying appropriate procedures in line with the potential losses at stake. The higher the risk, the greater the likelihood that a periodic rescreening of the entire customer base against a PEP list may be undertaken by some institutions. Alternatively, the process may be to review clients on an account by account basis against an agreed schedule or when a request for a new product or the opening of a new matter flags a potential risk. For many firms, relying on their relationship managers' knowledge of their customers' changing status is still key; however, given the increasing emergence of new regulatory and reputational risks, the most extreme policy may simply be to oblige customers to notify the firm if their status changes in line with any of the PEP categories outlined in the MLR 2007. This may be addressed through a standard clause within the terms of engagement approved by the client.

The impact of the economic downturn, heightened financial crime and persistent regulatory change all conspire to continue to make AML compliance a core area of focus for the regulated sector. How politically exposed persons are screened and subsequent business relationships monitored on an ongoing basis continues to be a central function within the AML process. Inevitably, those firms with the most to lose are adapting their policies accordingly, implementing new technology to flag early warnings of potential risk and putting proven AML processes and resources at the heart of an emerging enterprise risk model. Ultimately, whatever the approach, as long as policies and procedures continue to be proportionate to the perceived risk and demonstrate best endeavour, there is little more that can be expected.