

## **Overcoming Corporate Compliance Concerns**

*Tony Pullen, Experian*

UK businesses currently face revisions to the Anti-Money Laundering Directive. This article argues that integrated systems and automated authentication processes can ease the administrative burden of achieving compliance in the business-to-business arena.

Research from Experian conducted earlier in 2007 highlighted the fact that businesses in the UK were failing to tackle the issue of compliance with anti-money laundering (AML) legislation. The poll, conducted among anti-fraud, risk and compliance experts, found that 51% of corporates in the UK were at risk of being fined for failing to have adequate AML procedures in place. In addition, 49% were still relying on fraud-friendly paper-based authentication procedures to verify the identity of both individual and business customers.

### **Becoming AML Compliant in the Business-to-business Arena**

So what should businesses be doing in terms of tackling the issue of money laundering and what extra requirements will the new AML legislation place on them?

Existing Joint Money Laundering Steering Group (JMLSG) guidance on money laundering advises that, for corporate customers, a full name, registered number, registered office in the country of incorporation and a business address is required as standard evidence. In addition, for privately owned businesses, the names of all directors, and, where appropriate, beneficial owners holding over 25% of shares with voting rights needs to be verified. Politically exposed persons (PEPs), those who have had a high political profile or held high public office, also need to be authenticated.

However, from 15 December 2007, businesses will be required to authenticate the identity of all shareholders, where they are beneficial owners, in addition to directors and proprietors. By law, businesses will also be required to monitor relationships with their business customers and take a risk-based approach to due diligence and assessing what threats are posed to their business by the companies they deal with.

In addition to banks, financial institutions and other FSA regulated businesses already subject to Money Laundering Regulations, the revisions extend AML responsibility to a wider range of companies, including any organisation that accepts cash payments of €15,000 (around £10,500), or above, as well as casinos, lawyers, estate agents and accountants, regardless of the level of one-off cash payments they accept.

### **Integrated Systems**

On initial examination these extended requirements, and the enhanced level of due diligence they demand, would appear to put a considerable additional burden on UK businesses already struggling with a rising tide of legislation. But far from having to invest in specialist anti-money laundering solutions, compliance can be achieved by utilising the in-built AML functionality and electronic

authentication processes integral to systems that many businesses already use: those for processing commercial credit applications.

The largest organisations and even many smaller companies routinely use credit application processing systems to make decisions on which businesses to open or extend credit lines with and to assess the stability and commercial integrity of companies they transact with. These systems cross-reference a host of information databases and can highlight credit applications from suspicious businesses, disqualified directors or insolvent companies who are trying to trade illegally.

But they can also do so much more. Credit processing systems can deliver a high level of AML compliance for the business-to-business environment, as well as cost reductions and increased efficiencies for automated credit decisioning.

These integrated programmes enable businesses to achieve compliance with the enhanced regulations as they are able to automatically verify shareholders and beneficial owners, in addition to directors and proprietors in other businesses, as part of the commercial credit granting process.

Built-in electronic authentication automatically verifies the details of a business, while money laundering enhancements such as Know Your Customer (KYC) procedures and controls, checks against PEPs and checks against sanction files ensure businesses attain the highest level of compliance with the new regulations.

#### Electronic Authentication of Shareholders and Beneficial Owners

Electronic authentication means that by checking against powerful information databases, authentication screens can display the type of position the individual being checked holds, for instance, director, company secretary or shareholder, and whether a shareholder or company secretary is actually a company. Shareholders can be ranked by a percentage, based on the percentage total of issued capital where they have voting rights. For all displayed contacts, an authentication level, including 'not authenticated', will be given and a search against a PEP file conducted. Such PEP databases are important as they can highlight individuals who might potentially pose a higher money laundering risk to businesses as their position makes them vulnerable to corruption.

#### Sanction File Checking

Integrated applications can also provide a referral alert if a business' details are matched against one of eight sanction files or databases when a commercial credit application is processed. These include databases from the Bank of England's Financial Sanctions Unit, the Home Office, the European Union, the Home Office, the Isle of Man Financial Supervision Committee and Officials of OFAC blocked countries, and contain details of businesses that have economic, trade or financial sanctions imposed on them by governments or the United Nations. If a match has been found, a warning message is displayed at the top of the business report. Where no match has been found, a narrative will be displayed to confirm this, providing evidence that a search has been conducted.

In this way, such systems remove the need for separate AML checks to be undertaken, eliminating any additional administrative burden and leaving a clear audit trail. With the level of compliance they are able to deliver, organisations should seriously consider the benefits they can offer in assessing new business applications and simultaneously protecting their business from fraudulent activity in one integrated,