

Protection from money laundering with minimum impact

The implications for information professionals

Annalie Vickers

OneSource Information Services, UK

‘A legal professional is now held accountable as they “should have known or suspected” a client of money laundering. No longer is the law limited to just actual knowledge or suspicion.’

Annalie Vickers, Director of Product Marketing at OneSource Information Services, manages OneSource’s product portfolio for the European market. Annalie has worked in the information industry for more than nine years. She has been with OneSource for five years in a variety of product and content roles, including two years in the US head office. Prior to that she worked for LexisNexis. OneSource is a recognized leader in business information solutions. It aggregates and integrates information on over 3.2 million public and private companies, seven million executives and hundreds of industries worldwide. Combining and organizing this content from over 2500 information sources supplied by more than 35 world-class content providers, OneSource has created an unequalled information resource encompassing company profiles, corporate families, industries, executives, financials, news, analyst reports, and trade and business press articles. OneSource information is available using the web-based Business Browser business information solution or by integrating content directly into an organization’s existing systems, such as CRM, intranet or portal, using the OneSource AppLink Software Development Kit.

Abstract

The ease of transferring vast sums of money around the globe using computer networks provides opportunities for corruption. To help combat international terrorism and drug trafficking, the legislation relating to money laundering has recently been strengthened and extended to new business sectors. In this article we will explore the elements of the legislation that have changed and look at what information professionals can do to ensure that their systems are compliant while minimizing the impact and hassle-factor for clients, prospects and staff.

Keywords: criminal law, customer relations, ‘know your client’ checks, information professionals, legislation, money laundering, protection, layering, placement, integration

What is money laundering?

The official definition given by the National Criminal Intelligence Service (NCIS) is:

The various ways criminals conceal, move and legitimize the money they make from crime are described generically as money laundering, and tackling money laundering is fundamental to combating serious and organized crime.

Money laundering has been around for centuries and is now the world's third largest 'business'. While the fundamentals of this crime remain largely the same as in the days of Al Capone and the old Mafia, technology has offered, and will continue to offer, a more sophisticated and circuitous means to convert ill-gotten proceeds into legal tender and assets.

In Europe, the creation of the single market not only aids legitimate business, but may also provide increased opportunities for money laundering and financial crime. The UK Home Office estimates that £18 billion per year in 'dirty money' is cleaned by London's financial institutions and professional advisers, for criminal use. Corruption through money laundering has a potential impact on virtually every facet of life in a country – political, economic and social. The International Monetary Fund estimates that it is worth between two and five per cent of the global gross domestic product.

The primary purpose of organized crime is to make profits. Like any business, the purposes of profit are to enjoy it and re-invest it in future activity. For the organized criminal, however, profit close to the source of the crime represents a particular vulnerability, and unless the criminal can effectively distance himself or herself from the crime that is the source of the profit they remain susceptible to detection and prosecution. Hence the need to launder or 'clean' their illicit profits (usually though not exclusively through the financial services industry) to make them accessible and appear legitimate.

The legislation in context

To help combat international terrorism and drug trafficking, there is a raft of new domestic and international legislation, regulations and guidelines. Specifically in the UK, the legislation relating to money laundering has recently been strengthened through the Money Laundering Regulations 2003 and changes to the Proceeds of Crime Act 2002. Information professionals should know the legislation and how best to respond to it in some detail.

The new money laundering regulations came into force on 1 March 2004. The regulations were published in a statutory instrument, The Money Laundering Regulations 2003. The legislation, based on an existing European Directive, widens the scope, so that the responsibility of reporting money laundering activity is

extended beyond the banking sector to include auditors, accountants, tax advisers, insolvency practitioners, legal professionals, real estate agents, dealers in high-value goods and casinos. Dealers in high-value goods could be any business that supplies goods and accepts large payments of 15,000 or more for them, in cash.

In addition, the offence of money laundering is governed by revisions to the Proceeds of Crime Act 2002 that took effect from February 2003. Previously the law was limited to money laundering activities involving drug trafficking, terrorism or serious crime. The new regulation relates to *any* criminal activity. For example, a legal professional is now held accountable as they 'should have known or suspected' a client of money laundering. No longer is the law limited to just actual knowledge or suspicion.

Under the Proceeds of Crime Act, a money laundering offence is committed by any person who conceals, disguises, converts, transfers or removes from the UK criminal property. A third party commits an offence if they enter into or are connected with a business arrangement which they know or suspect facilitates the use of criminal property by or on behalf of another person. However, the third party does not commit an offence if they disclose the suspected use of criminal property or can prove that they intended to disclose it. The penalties are a fine or imprisonment.

Finally, at a European level, the EU Data Protection Directive requires each member nation of the EU to protect all personal information that is collected against accidental or unlawful destruction, loss, alteration and unauthorized access or disclosure.

With the EU Data Protection Directive, information professionals have to be aware of all the information they hold on clients and prospects, how that information was collected and how it is stored and used. This requires a strong understanding of the difference between public domain information and personal information that is protected by the Data Protection Directive. Working with experienced information vendors, like OneSource, with experience in aggregating public data from trusted and quality sources is vital to meeting this directive.

A key part of all this legislation is the requirement for 'Know Your Client' checks that interrogate key financial information on companies and their directors, provide an audit trail of what has been done and report on suspicious activity. The Financial Services Authority

(FSA) states that ‘one of the main purposes of ‘Know Your Client’ is to help businesses to manage effectively their money laundering risks, by reducing the likelihood that they will take a money launderer as a customer and increasing the likelihood that they will detect the use of their products or services for money laundering’. This is a resource-hungry task for many companies and will require significant management by information professionals. The ‘know your client’ processes are seen by the FSA as the most effective prevention against money laundering.

Changing relationships

The British Chambers of Commerce revealed that since 1997 compliance costs have risen to £30 billion. As a result the customer-vendor relationship has been changed, particularly in the early stages. As part of implementing the new legislation we must be careful to protect the trusted client/supplier relationship, while ensuring that laundering is driven down.

In order for business to take on the role of gathering the right data to ensure compliance (but that this task doesn’t end up eating up valuable resource and budget), businesses need some simple processes to follow that ensure gathering information is part of normal business practice, and not an onerous task. Information professionals will need to source information on customers, prospects and partners to help comply with the ‘Know Your Client’ part of the new legislation as well as reduce operational risk.

Your obligations

1. Money service operators and high value dealers are required to register with HM Customs and Excise. High value dealers have only been required to register since 1 April 2004.

2. A report must be made to the NCIS if you believe that something you come across, in the course of your profession, involves criminal conduct and represents funds or property that derives from a criminal offence (or something that occurred overseas and would be a criminal offence had it taken place in the UK).

3. It is important to remember that breaching the requirements of the legislation could lead to significant criminal penalties.

4. All organizations that carry out the relevant business must have systems and training to prevent money laundering and set up identification, record keeping and internal reporting procedures.

5. It is recommended that a money laundering reporting officer be appointed to receive reports of suspicions and channel these to NCIS. The new regulation will affect the way firms covered by the legislation do business. In some businesses the regulations will also create a new requirement for information.

As a further preventative measure, the identity of new clients should always be verified. In the case of a business relationship with an individual, the standard identification procedure is to ask to see a passport or driving licence and a recent utilities bill. Addresses can be double-checked against the electoral register. Information on individuals can be obtained from credit databases. Further information can be found on individuals who are company directors, such as details of multiple directorships or an association with failed companies. A press or Internet search may produce valuable information, but is time consuming. Information professionals will need to undertake a review of their suppliers and make sure that they are being given access to everything they need to comply.

Out with the old and in with the new?

Most companies will already have some form of process in place to allow for the sourcing and use of information as part of customer management and knowledge management systems. In the legal sector for example, gathering information on a customer’s financial history has always been a central part of ‘due diligence’. Insurers too are likely to have systems in place to analyse the commercial risk for existing and prospective customers.

These systems, in whatever form, will make complying with this legislation easier and mean the role of the information professional is one of evaluation and updating.

What have you already got?

Firstly, ask yourself some key questions about the information you have:

- Does it provide sufficient information on the company and the industry it operates in?
- Can you determine if the external entity is involved in money laundering?
- Is it clear if it is part of a parent company and what other companies are involved in the parent?
- Can you see who all the key directors and shareholders are?
- Can you view debt records (county court judgments, mortgage arrears or charges for example)?
- Is the company publicly listed? If so, is it on a regulated exchange?
- Is the company a subsidiary of a publicly listed parent?
- Is the company well known and long established?
- Are there any institutional shareholders with less than 20 per cent share capital?
- Are any directors or shareholders on sanctions lists?
- Does that individual or organization have sanctions or enforcement actions against them?

The next step is to look at how you are gathering this information. A series of manual checks at various stages of the initial dealings with new customers – a client acceptance process for example – is the ideal business process in which the information needs come together.

Sourcing the right information

For many companies ensuring compliance will require increasing the business information that they have access to. As most information professionals know, it's far more productive to use an information provider that delivers quick and easy access to the information that they need – directly from the desktop.

Companies with the right processes in place will be able to comply, and prove compliance, with new

legislation. A simple system that provides access to the right information at the most appropriate stage of the client contact will be the most cost-effective.

Some information vendors provide a tailored service that will assist in the client checking process. These vendors will be able to provide reports that include the key information on:

- company details
- share capital and shareholders
- directors and secretary details
- mortgages and charges
- adverse information on liquidation, receivership, administration or winding-up notices
- directors' details including home address, date of birth, nationality, other directorships
- shareholders' details including address, and number and par value of shares held
- group structure (information on subsidiaries)
- financial history
- gearing, liquidity ratio
- outstanding county court judgments.

Increasing productivity through integration

To increase productivity further, the required information can be integrated directly into business systems and processes. For example, in the insurance industry information can feed directly into the existing risk assessment process. And in the legal sector, it can form part of the existing due diligence procedures.

Some systems can be integrated into an organization's existing workflow. This means that you can:

- search and classify companies according to a risk profile
- review the corporate family structure of prospects, clients and partners

- create an audit trail of money laundering investigations
- choose pass/fail criteria for anti-money laundering checking
- check the backgrounds of a company's directors and shareholders
- review financial filings and exchange listing details
- choose pass/fail criteria for anti-money laundering tracking
- receive risk level classifications and direction on further analysis required.

If necessary, you can also gain access to databases of people who are suspected or known terrorists, drug-traffickers, arms dealers, money launderers or financial fraudsters.

Whatever system or service you choose it is essential to fully understand the diversity and quality of information that you are buying, the scalability of the solution for your business and the integration possibilities into your existing processes and procedures. When the system is in place, businesses must be careful not to be complacent. The new legislation's 'Know your Client' element is reflecting the necessity to understand business patterns and behavioural aspects of your client and take some responsibility for spotting anything that you perceive to be unusual. Integrated systems undoubtedly help to achieve this.

Keeping customers happy

At the end of the day you are in business to serve your customers and their needs. We have all experienced the seemingly unnecessary questions that come at the start of a business relationship or personal relationship with a financial institution or adviser.

To keep your customers happy the more you can do to facilitate simple and clear exchange of information the better. Be clear that this is to protect them and their money as well as you – it is of mutual benefit. Don't let your staff complain about or belittle the process.

However you approach the legislation, you will need to refine your processes for gathering and evaluating the knowledge necessary to comply with regulations, but also to improve the organization's risk posture.

A system that can check for all of these criteria automatically will save time and put the information where it's needed. Further, an automated system will help prove that you've got sufficient processes in place to comply with the legislation.

Manual processes for gathering information are likely to be labour intensive and costly. A process that is too long will not help compliance. Moreover, it could also slow down new customer dealings, which is not good for any business.

The bottom line

Billions of 'dirty' pounds are mistakenly 'cleaned' by financial institutions and professional advisers, or received by businesses turning a blind eye to large cash payments. As a consequence, money laundering represents a serious threat, not just to sound economic and financial development but to the political integrity and

How do money launderers do it?

According to HM Treasury's Money Laundering Strategy, there are three internationally recognized phases to money laundering: placement, layering and integration.

Placement occurs when the cash generated from the crime is placed in to the financial system or used to buy goods. This is the point at which the proceeds of the crime are at most risk of detection. At this point the dirty money is most likely in cash. Those seeking to deposit it will target banks, cash businesses or dealers in high-value goods.

Layering is where dirty money passes through a series of transactions in order to obscure the origin of the proceeds. These transactions may involve trusts, share or insurance products across multiple jurisdictions. Smurfing, according to the NCIS, is the terminology used to describe the breaking down of a large amount of money into smaller amounts that fall beneath the financial institution's radar.

Once the original source of the fund has been obscured the final stage is for the money to reappear as legitimate fund or assets. For example, income through a business. This is known as **integration**. The criminal is then free to enjoy the proceeds of the crime with much less fear.

The Financial Action Task Force (**FATF**) on Money Laundering has identified certain 'choke' points in the money laundering process that the launderer finds difficult to avoid and where he is vulnerable to detection. The choke points identified are entry of cash into the financial system, transfers to and from the financial system and cross-border flows of cash.

stability of our nation. I would urge all information professionals to play their part in ensuring their business has the right systems in place to help them 'know their clients' better and hence combat international crime and protect the assets of their business and its customers.

Further information

HM Treasury: www.treasury.gov.uk

The Financial Services Authority: www.fsa.gov.uk

HM Customs & Excise: www.hmce.gov.uk

Home Office: www.homeoffice.gov.uk

Assets Recovery Agency: www.assetsrecovery.gov.uk

National Criminal Intelligence Service: www.ncis.co.uk

AccountingWEB: www.accountingweb.co.uk

Institute of Chartered Accountants in England & Wales: www.icaew.co.uk

Experian: www.experian.com

Equifax: www.equifax.com

How to obtain copies of the legislation:

Money Laundering Regulations 2003: www.legislation.hmso.gov.uk/si/si2003/20033075.htm

Proceeds of Crime Act 2002 – Part 7: www.legislation.hmso.gov.uk/acts/acts2002/20029-k.htm

Terrorism Act 2000: www.legislation.hmso.gov.uk/acts/acts2000/20000011.htm