Microsoft Financial Services White Paper
Compliance

May 2005

Anti-Money Laundering Compliance

Microsoft
Your potential. Our passion.™

Contents

Acknowledgements

Microsoft would like to offer its thanks to the following people and organisations for contributing to and assisting in the production of this white paper:

Kalypton Limited

Lars Davies, Consultant, Kalypton Limited

NetEconomy, a provider of enterprise risk monitoring solutions for anti-money laundering and fraud detection

Introduction

In the first paper in this series on compliance, the opening statement defined compliance as 'meeting all the legal and regulatory obligations that a commercial concern faces.'[1]

Anti-money laundering (AML) compliance is another example of a legal obligation placed on any person or organisation. Financial services professionals have a duty to report a suspicious transaction although detailed record keeping requirements are currently only defined by the financial sector regulators.

Money laundering controls and regulations are seen as fundamental in the fight against terrorism and organised crime. In addition, prosecutors are increasingly using money laundering as a charge when prosecuting firms and individuals for breaches of securities regulations.

Although regulations vary between jurisdictions, they have as a common basis the need to carry out customer due diligence – 'know your customer' (KYC) – and the ability to demonstrate that this was carried out. This is achieved by generating specific records and maintaining these records for a significant period of time, in one example for at least five years after the client relationship has come to an end.

A further requirement is, except in certain specified circumstances, to report any suspicious transactions to the authorities. Organisations also now have a duty to educate their staff to be able to recognise such transactions.

Regulated organisations are being fined heavily for not only failing to keep the correct records but also for their inability to retrieve records to the satisfaction of the regulator. They have also been fined for failing to provide notification of suspected fraud in a timely manner. This is despite the records being generated and no specific evidence of laundering taking place. The failure to keep and retrieve records alone was the problem.

Organisations should be wary of solutions that only claim to meet a narrow selection of regulations. A compliant solution must meet all the underlying requirements upon which the specific regulations are built. If a solution cannot meet the underlying requirements of a regulation then it cannot support that regulation.

1 Please see Microsoft's Compliance Overview white paper published July 2004

Increased Sophistication and Increased Regulation

The global nature of money laundering has rendered geographic borders irrelevant as launderers move funds between jurisdictions where their activities are more likely to go undetected.

Over the last few years, particularly in the aftermath of September 11, it has become clear that laundering is a collective, dynamic activity that should not be viewed as a single act, but as a clever and complex process.

One of the most publicised cases, that of former Nigerian dictator General Sani Abacha, highlights the complexity of laundering operations. It is believed Abacha looted some $3bn from state finances. An FSA investigation into the handling of accounts identified 42 personal and business bank accounts held at 23 banks in the UK alone linked to the Abachas. The regulator ordered seven banks to immediately tighten their controls or face unlimited fines and public naming.[2]

As such, money laundering has become universally regarded as a major operational risk for financial institutions. The damage a launderer can cause reaches beyond law suits and regulatory censure. Any organisation, or individual, caught up in a laundering scandal can find their reputation as well as their career irreparably damaged.

Governments worldwide are making concerted efforts to enforce existing legislation, introduce new, more stringent penalties and name and shame those in non-compliance. Their scope has evolved from what had previously been deemed 'best practice' or 'guidance' into law, while changing the legal definition of money laundering.

Basel II, The USA Patriot Act, the EU Directive on Money Laundering and the revised recommendations of the Financial Action Task Force have increased the global extent of anti-money laundering (AML) regulations. The UK has also extended regulations under Part 7 of the Proceeds of Crime Act[3] to cover lawyers, accountants, casinos and estate agents.

Financial institutions have become the first line of defence, which means the board of directors, as well as individual executives, are now responsible for ensuring compliance.

The USA Patriot Act in particular has come to prominence due its strict requirements on institutions. It sets out a number of provisions that institutions should look for when evaluating money laundering systems.

It requires financial institutions to establish anti-money laundering programmes that, at a minimum, establish: internal policies, procedures and controls; a designated compliance officer; an ongoing employee training program; and an independent audit function to test programs.

For example, Section 326 of the Act requires firms to establish a customer identification program and maintain records on customer identification, including the methods taken to verify a customer's identity.

This has already impacted on correspondent banking relationships in the US, with respect to new information, due diligence and reporting requirements. It is also applicable to any UK regulated firm that has a parent, branch or subsidiary in the US, or has a financial relationship with an institution in the US.

2 FSA Press Notice 029/2001: http://www.fsa.gov.uk/pubs/press/2001/029.html
3 http://www.legislation.hmso.gov.uk/acts/acts2002/20029--k.htm

Beyond US federal legislation, groups such as the Basel Committee and the OECDs Financial Action Task Force (FATF) have introduced increasingly severe regulations.

The FATF, an inter-governmental body that fosters the creation of a worldwide AML network, has developed a blacklist of Non-Co-operative Countries and Territories (NCCTs). These are jurisdictions deemed to be not doing enough to comply with FATF directives and this is already having an impact, with these territories being ostracised from the financial community.[4]

The FATF's 40 recommendations strengthen customer due diligence and record keeping requirements and suggest the adoption of a risk-based approach to AML activity.

The revised recommendations also suggest that laundering is not confined to the banking sector. They require countries to establish systems to ensure that adequate beneficial owner information is obtained, verified and recorded for corporate vehicles such as private limited companies, bearer shares and trusts.

These records should be retained for a minimum of five years after an account is closed or relationship ended, to enable transactions to be reconstructed and the documents used as evidence in criminal prosecutions.

[4] Current NCCTs are: Cook Islands, Egypt, Guatemala, Indonesia, Myanmar, Nauru, Nigeria, Philippines and Ukraine. http://www.fatf-gafi.org/NCCT_en.htm

UK Perspective

There are four principle sources of authority with regard to money laundering in the UK – the primary legislation, the Money Laundering Regulations, the FSA Rules and the Joint Money Laundering Steering Group Guidance Notes (JMLSG).

These have introduced five basic money-laundering offences:

- **Assisting another to retain the benefit of crime;**
- **Acquiring, possession and use of criminal proceeds;**
- **Concealing or transferring proceeds to avoid prosecution or a confiscation order (also called Own Funds money laundering);**
- **Failure to disclose knowledge or suspicion of money laundering;**
- **Tipping off.**

Since December 2001, when the FSA received its new legislative powers, relevant firms have also been subject to a general requirement to establish and maintain effective systems and controls for countering risk that the firm might be used to further financial crime (SYSC 3.2.6R).[5]

The FSA's Money Laundering Sourcebook[6] requires that institutions:

- **Set up procedures for verifying the identity of clients;**
- **Set up record-keeping procedures for evidence of identity and transactions;**
- **Set up internal reporting procedures for suspicions, including the appointment of a Money Laundering Reporting Officer (MLRO);**
- **Train relevant employees in their legal obligations;**
- **Train those employees in the procedures for recognising and reporting suspicions of money laundering and raise awareness of their responsibilities under company AML policy.**

Under the Sourcebook, financial institutions are responsible for policing their financial dealings and reporting any suspicious transactions, including any over the threshold of £10,000.

If an individual knowingly aids a launderer, or if a transaction, client or colleague causes them to suspect laundering and they fail to report their suspicion, they can be held personally responsible. For example, 'tipping off' someone that they are under investigation is an offence and punishable by up to five years imprisonment.

Recent high profile cases reflect the degree of importance the FSA attaches to AML systems and controls being in place. Abbey National companies were fined a total of £2.32m for serious compliance failings, including breaching the FSA's Money Laundering Rules and systems and controls breaches.[7]

The FSA rules require firms to generate and retain records of customer identification because these are vital to the investigation, detection and prevention of financial crime. Bank of Scotland was fined £1.25m for failing to keep proper records of customer identification. "The size of the fine demonstrates that failure by firms to put in place and maintain effective systems and controls will be dealt with severely by the FSA," says Andrew Procter, FSA director of enforcement.[8]

Can you say with any certainty that you know the identity of the customer, or that your systems can identify, track, record, store and report these transactions effectively? If not, your organisation could join those that have received substantial fines and the subsequent adverse publicity.

5 http://www.fsa.gov.uk/vhb/html/SYSC/SYSC3.2.html
6 http://www.fsa.gov.uk/vhb/html/ml/MLtoc.html
7 http://www.fsa.gov.uk/pubs/press/2003/132.html
8 http://www.fsa.gov.uk/pubs/press/2004/001.html

A New Approach to AML Compliance

Meeting new anti-laundering requirements should not be viewed as merely a compliance issue, but a broader governance and enterprise-wide risk management issue.

Although legal requirements and loss of reputation are the drivers for many institutions to adopt new processes and systems, those thinking strategically can exploit the opportunity to gain greater business benefits.

Detecting suspicious transactions is not a simple task. The introduction of new payment channels, Internet banking, and wireless transactions has made attaining and maintaining this information even harder.

A number of principles are recognised as central to any AML programme:

- **Compliance with the relevant AML laws of the appropriate jurisdiction;**
- **Know your customer, including the source of their wealth;**
- **Co-operating with various law enforcement and supervisory agencies;**
- **Communicating the AML programme through policies, procedures and staff training;**
- **Continuous and sustainable money laundering risk-assessment across the enterprise;**
- **Secure records storage and management with full audit.**

The immediate response by many financial services firms has been to bridge any obvious flaws in their processes while struggling to remain compliant with an array of international anti-money laundering regulations, lists and recommendations.

However, financial services firms are taking a step back and realising that a competitive advantage can be achieved by developing a comprehensive, strategic response to the growing threat of money laundering.

This requires senior management to devise a strategic approach through a comprehensive review of the business model and the risk of laundering in specific products, business lines, geographies and subsidiaries.

Traditionally, the response has been to review the systems and controls issues identified after an event has exposed a particular flaw. Management now need to become proactive and create a framework for implementing systems and controls to monitor transactions that enables staff to recognise and report suspicious transactions.

Adopting a long-term vision when formulating an AML strategy can act as a catalyst to re-engineer the business model to achieve compliance and incorporate a system and strategy that supports wider business needs.

Visionary boards who adopt this strategy will find the approach a powerful tool in driving out organisational barriers to create an agile and flexible business.

Enterprise-wide Intelligence

The biggest hurdle for many AML systems surrounds data. Banks have to detect, track, extract, warehouse and gather data to gain an insight into customer behaviour and identify any suspect transactions or patterns.

An underlying problem is the ability to demonstrate that the correct records have been captured, created and stored in such a way that they can be retrieved on request by authorised officers.

This places another specific requirement on the corporate compliant solution outlined in the previous white paper.

To achieve this, banks require a solution that can evaluate and analyse transactions at a deeper level of detail, within the context of each customer's behaviour and that of peer groups across the institution.

With the sheer volume and complexity of transactions handled by large financial institutions, the detection of suspicious transactions has to be undertaken by a sophisticated, automated solution.

Traditional monitoring systems utilise a rules-based approach, designed to detect certain laundering behaviours rather than suspicious transactions. These normally involve loading various scenarios in which a launderer can launder money through an institution and create rules in a solution to detect transactions that fit this pattern.

However, a rules-based approach does not detect much of the laundering activity that occurs within an institution, as laundering patterns are not easily discernable.

"The obvious flaw is that if you can think of a rule based scenario, so too can a launderer and the chances are they already have," says John Bone, Sales Director, UK and Ireland, NetEconomy. "As scenarios, financial products and the customer base change, so do the rules, which leads to an on-going maintenance issue. It is a similar problem with neural networks, in that you have to retrain the neural networks as your business environment changes."

Moreover, inaccurate or unspecific rules tend to produce a high number of false positives – transactions labelled as suspicious that do not represent a laundering risk. Without any explanation of these alerts an already stretched compliance department can become overwhelmed, taking their focus off transactions that represent a greater risk and possibly leading to wrongful follow-up. This can endanger the financial institution's relationship with the customer.

New regulations demand that businesses adopt systems with greater analytics. A compliant system needs to combine rules-based and advanced analytics to provide adequate protection from increasingly skilful launderers.

Intelligent Enterprise Systems

An enterprise-wide, or 'intelligent enterprise', solution looks for any form of unusual behaviour as opposed to looking for specific patterns or forms of laundering.

It monitors accounts and their interaction to encompass deposit methods, frequency, and volume of money to build a complete transaction picture.

By taking an enterprise-wide approach institutions can determine what is normal and what is unusual for each customer and account. This enables institutions to make more informed risk assessment and identify known and emerging laundering schemes.

This approach was a critical factor for one of NetEconomy's biggest users, Nationwide, which has 11 million members. It needed to monitor up to three million transactions per day, and required a system that delivered high-quality, targeted alerts to its AML team.

"You can look at account history or use peer group comparisons to try to establish any unusual behaviour. A small business operating out of a Reading postcode should have a similar profile of account activity as another small business operating in the same area, using similar banking products," says Bone.

This enables institutions to have a continual analysis of the transaction, while the system has the ability to learn and understand each profile and detect links between seemingly unrelated actions.

"A big advantage is that you can tweak this type of system to place rules above it to look at known scenarios," he says. "But, by its nature if people change the way they launder money the system will inherently pick that up as a break from normal account activity. It tries to understand the customer and their activity, rather than artificial intelligence, which tries to understand the launderer."

The technology can incorporate multiple data inputs, from internal account data, customer information from a customer information system, and lists such as OFAC, Bank of England, and the FATF.

Matching algorithms within such a system can be specified to provide thresholds, for example an 80 per cent name match and 100 per cent postcode match to bring up an alert. Shortcuts to investigations could also be made by automatically reporting a 100 per cent hit from the OFAC list, while an 80 per cent hit can be sent to the investigations team for further analysis.

While such unique transaction monitoring capabilities are complex, combining multiple techniques, including profiling, peer-group analysis, and rules, the result is simple: fewer, more accurate alerts. With higher hit rates the compliance team can spend their resources on only the activity that is worth investigating.

"It's really about educating institutions that it is not a case of simply raising alerts," says Bone. "In a reasonable sized bank there will be between two and five million transactions per day that have to be analysed. One of the most important factors is how you manage that into the number of alerts you present to operators and the quality of those alerts. Our experience with existing customers such as Nationwide suggests that."

Efficient Workflow and Case Management

With a suspicious transaction detected, the investigations team need to begin the arduous task of data mining. This will determine whether a report should be made to the National Criminal Intelligence Service (NCIS).

Critically, not all unusual activity is laundering. For example small businesses may use current accounts that will result in a lot of money moving through what is generally considered a low cash flow product.

"What you have to do within a system is to provide a set of tools that enables the user to determine whether that unusualness is suspicious," says Bone. "That could be using graphical analysis to understand the individual transaction over time, or where the funds are coming from. It may well be that they've sold a car for cash, but then you might ask how many cars they have sold, which could be a cover for putting cash through an account."

Efficient workflow and case management are critical to achieving an enterprise-wide solution. With a centralised system a rich information store can enable better detection and quicker investigations.

To satisfy regulators that appropriate measures have been taken, this process must be fully auditable and enable institutions to maintain, retrieve and report activities. The presentation of suspicious activity in a user-friendly manner is crucial, as investigations tend to be a manually intensive process.

However, without a centralised enterprise-wide AML solution an institution will not have the visibility to know precisely what is happening within its business, or when. Institutions need a case management system enabling compliance officers to organise, prioritise and manage the investigations.

"Case management capabilities are vital and a lot of the recent FSA fines have been down to this and a lack of visibility to what is happening within an organisation," says Bone.

If a company cannot actually access that information, then in legal terms it is as if that information was never retained in the first place.

This makes workflow a crucial aspect to prove that the correct records have been captured and stored in such a way that they can be retrieved when requested by the regulator. Institutions have to demonstrate the evidential weight of records if they are relied upon in a prosecution.

Once a case is opened, firms must continue to retain all the documents sent between customers, counterparties, or third parties. A variety of supporting documents could be attached to a case, including correspondence in the form of emails or letters, scans, and images.

All of this information needs to be stored in a data repository as an electronic case file that, should the need arise, can be sent to the regulator. The authenticity of electronic documents is critical for compliance and audit trails need to show when conversion took place and whether any changes were made.

Additionally, with the complete case history, including all transactions, a detailed log of all actions taken and reports filed should be automatically recorded for review by operations managers and the FSA.

There is also the question of how much data you store in order to detect laundering and how much you subsequently keep for investigations. "Archiving is crucial as it usually involves terabytes of data, but with the technologies available in products such as Microsoft's SQL Server, there doesn't seem to be an issue here," Bone says.

"In a multi-user system you have levels of security and logging built in. So, when there is an alert, it is placed in a queue and an operations manager may delegate this to an investigator," he says. "During investigation, if a letter is sent out to a customer by the investigator, that also has to be put into the database and it all has to be auditable – who did what, when, why and what actions resulted from that."

"The tracking stage of a system is collating relevant information into a single case management system, where you can perform an investigation, collect evidence and build a case against an account holder, which can then be reported to NCIS" says Bone. "If the FSA comes to you in a year and looks at the history of the case you can show why it was reported along with the case history, or in some cases why it was not reported."

This covers not just centralised alerts, but also those suspicions raised by branch staff that need to be entered into the system. A solution can be deployed via a Web interface so that all manual suspicions are also entered.

This enables an institution to have a centralised, enterprise-wide tool for all AML cases, not just those automatically created by the software ensuring all suspicious activity is captured.

Conclusion

Money laundering poses a significant and growing risk to financial institutions. Regulators globally are clamping down on those institutions that cannot prove, to their satisfaction, that they have in place systems and controls to stem the flow of illicit funds.

It is also another example of a regulation that places significant record retention requirements on those industry sectors that are subject to it.

The process of obtaining, processing and storing data associated with AML compliance is an arduous task for financial institutions already struggling with the terabytes of data produced by their day-to-day business.

This makes attempts to pull this information from disparate systems, analyse and act upon it even harder. However, the challenge of AML compliance also represents a tremendous opportunity for financial institutions to implement a solution that introduces cost-effective and efficient technology into daily business processes.

A combination of comprehensive monitoring, case management and suspicious activity reporting via an intelligent enterprise system can provide a broad defence against money laundering. Providing a strong platform for AML allows financial institutions to expand their monitoring capability to other areas of the business such as Fraud and Market Intelligence.

However, without the introduction of such solutions, the task will only become more difficult as launderers use increasingly sophisticated methods to clean the proceeds of crime.

This can leave an organisation open to attack and the risk of their reputation being tarnished and therefore shareholder value, or in the case of mutual organisations, member's confidence, damaged.

As an organisation carries out efforts to become compliant, it must ensure that a solution is capable of meeting the money laundering record retention requirements as well as the stringent data protection requirements that this involves.

Meeting the requirements of compliance cannot be seen as an option, it is a cost of doing business.

Is your organisation compliant?

For Further Information

If you would like to contact the Microsoft UK Financial Services team please e-mail:
fsindust@microsoft.com

For more information about Microsoft in Financial Services please visit:
www.microsoft.com/uk/financialservices

For more information about Microsoft in the UK, please visit:
www.microsoft.com/uk

NetEconomy, a provider of enterprise risk monitoring solutions for anti-money laundering and fraud detection
www.neteconomy.com

Kalypton Limited
www.kalypton.com

www.microsoft.com/uk