

**complinet**



[www.complinet.com](http://www.complinet.com)

Executive Whitepaper

## **How can you really know your customer?**

---

[The regulatory and business drivers of transaction monitoring](#)

---

May 2008

## How can you really know your customer?

Some years ago, a well-known charge card company coined a phrase as part of an advertising campaign which said:

*"Says more about you than cash ever can!"*

The company, of course, meant that the mere possession of its charge card made a statement and imputed some extra quality about its customers.

In this phrase, however, the advertisers came closer to the truth than their copywriter might ever have realized.

It is an old detective's adage that if you really want to climb inside the soul of a man, all you need to do is analyze his bank account. An investigator can gauge a person's state of mind most accurately by looking at the way that person directs their financial affairs.

The law states that when compliance officers set up systems and controls to deal with money laundering and other financial crime, they must monitor transactions and take a 'risk-based approach' in the process.

These phrases are more quoted than observed and they mean many different things to many different people.

In this paper we shall set out the meaning of the phrase 'risk-based approach to compliance' and show how useful transaction-monitoring systems are with helping compliance staff decide whether certain transactions warrant a suspicious transaction report.

## What is Transaction Monitoring?

Compliance departments have been monitoring transactions for a long time now. The Basel Committee on Banking Supervision made the first real allusion to transaction monitoring in 2001.

*"Banks should not only establish the identity of their customers but must also monitor account activity to identify those transactions that do not conform to the normal or expected transactions for that customer or type of account."*

[Basel Committee on Banking Supervision, 2001, "Definition of transaction monitoring for the purposes of achieving 'best practice' KYC."]

The committee viewed transaction monitoring as a method by which banks could spot frauds that were being committed against them, and be better-equipped to forestall losses. It was also examining the system's possibilities to combat financial crime more widely.

In July 2007, the Financial Services Authority issued a paper entitled 'Automated Anti-Money Laundering Transaction Monitoring Systems', in which it stated:

*"The draft Money Laundering Regulations (implementing the Third [European] Money Laundering Directive) will be laid before Parliament in the coming weeks. The regulations will make transaction monitoring (TM) compulsory. More specifically, firms will have to conduct ongoing monitoring of a business relationship, focusing both on scrutinising transactions and keeping the documentation and customer information up-to-date."*

Many institutions had long been using AML detection devices by this stage. KPMG reported in 2004:

*"Enhanced transaction monitoring is the main area of increased AML spending. Transaction monitoring activity has been the main cause of increased AML spending over the past three years; respondents anticipate that it will also be the main area of AML expenditure over the next three years. The challenge all banks now face is to build on and enhance existing systems. In doing so, banks need to continue to use a risk-based approach, assessing the relative risks that they face from individual products, relationships, and jurisdictions."*

KPMG Report on Global Money Laundering 2004

By this stage a number of software houses were offering products that claimed to identify potentially 'suspicious' transactions. In many cases, though, their claims were unrealistic. They said that their systems were 'intelligent,' that they could 'teach themselves'; or that they used 'neural networking,' whatever these claims were meant to mean. As a result, some very large Tier 1 banks paid significant sums of money for products that did not work very well and were incapable of growing along with regulatory demands.

The meaning of transaction monitoring was not fully explored because the answer was too simple for most providers' business models whose sales relied, all too often, on a combination of smoke and mirrors.

The following definition is a reasonable one:

Transaction monitoring is the act of monitoring day-by-day transactions [of whatever kind] that occur in an account, with the aim of identifying important changes in patterns of unusual account behavior. The further aim is to investigate them to ascertain whether or not they can be classified as 'suspicious' and disclosed to the relevant authorities.

Systems not only look for transactions that might be thought suspicious but also look for transactions above certain government-inspired thresholds, or transactions that might pertain to terrorism. They also ought to be able to look for risky transactions linked to patterns of behavior, "high risk" jurisdictions, politically exposed persons, etc. Any system that does this must be capable of doing the following:

#### **A statistical analysis and profiling of transactions that have to be detected**

- ▶ Banks must now report 'patterns' of behavior that underlie the transactions they are reporting. This is to help them explain why certain transactions are unusual or suspicious.
- ▶ They need systems capable of producing regular periodical reports and generating relevant statistics.
- ▶ They need to be able to provide 'exception reports' or 'investigation alerts' which are triggered off whenever transactions exceed certain set amounts.

#### **The monitoring of business to ensure that it does not ignore government watch lists**

- ▶ Banks must now buy checklists (of known terrorists etc.) from external software firms and integrate them into their own monitoring systems.
- ▶ Systems must be able to take account of changes in these name lists, and ensure that entities on the lists are not customers already.

#### **A search for names that appear again and again throughout the history of payment stored in the system**

- ▶ The system must be capable of applying fuzzy-matching techniques to identify names which may appear to sound similar when spoken phonetically, but which are spelt differently.
- ▶ Such a system must also be capable of analyzing such patterns of names to ascertain whether they are indeed related—either by blood or business attachment.

#### **The generation of reports to the government, complete audit trails and the aggregation of information and support for investigation alerts/exception reports**

- ▶ All transaction reports must now be transmittable to the financial intelligence unit in question electronically and must possess pre-populated formats, i.e., fields that the system fills in automatically.
- ▶ The system must generate annual audit trails for all transactions and reports to the financial intelligence unit. The money laundering reporting officer should be able to see every transaction and suspicious transaction report to which a certain transaction is linked.
- ▶ The TM system usually draws data from several other systems. The MLRO must be able to trace every investigation alert/exception report back to the system it came from.

## The pitfalls of most Transaction Monitoring systems

The primary responsibility of any MLRO is to tell the relevant FIU about any suspicious activity which is brought to attention. The officer is entitled to gauge the veracity of any report made by any member of staff to establish whether it should be reported. This is why, in the first instance, any report made to the MLRO should be of an activity or transaction which possesses 'unusual' or 'abnormal' characteristics. It is up to the MLRO to say whether such an activity or transaction is also 'suspicious.'

In making that determination, the MLRO should apply many elements of their own product knowledge, training, experience, and business acumen, but their ultimate guide must be their own knowledge of the client's financial and business conduct. The officer must know whether the transaction in question fits the client's normal or expected behavior, or whether it is too far out of the profile without any reasonable explanation.

Most transaction monitoring systems still make two fundamental errors. The first is that too many of them believe that their main purpose is to identify examples of money laundering and money launderers, whereas their legal duty in all EU countries is to determine potentially suspicious financial activities or transactions. They do not need to articulate the reasons for the suspicion, any more than they need to enumerate the specific crimes to which they think the transactions apply.

Secondly, too many of the IT systems on the market seek to make use of pre-defined characteristics that they mistakenly believe to represent the activity or identity of a money-launderer. IT solutions firms program their systems with complex models to detect determined criminal conduct.

Let us not be too surprised. It is in the interests of IT providers to make their products ever more complex (and thus more expensive) and to keep designing these systems to confront a growing number of patterns of activity. This, of course, enables them to maintain a constant flow of upgrades.

## How to take a risk-based approach towards money-laundering control

The MLRO who takes a risk-based approach to their job has to make certain assumptions and then apply them when estimating the level of risk that pertains to their institution's business and the clients that it serves. The 'risk' the MLRO is assigning to that business and those clients is often called 'money laundering risk,' i.e., the risk that some official body—perhaps a court or a regulator—will punish their institution for a reason or on a pretext that has something to do with money laundering.

The Government requires financial institutions to gauge this 'risk.' In setting out their risk-based approaches, they must identify risks, quantify them, and set out a strategy for mitigating them. The entire structure of systems and controls must be set out in an internal policy document. In some countries the institution must ask its regulator if it agrees with the document and it then becomes the subject of a signed contractual agreement between both parties.

The institution then has to keep showing its regulator that it is following the control strategy to which it has agreed faithfully. In future, the regulator will measure the institution's compliance according to its adherence to the risk-based approach agreement, not to its success in staving off money launderers. Transaction monitoring, with the initial aim of rooting out unusual financial transactions or activities, is a vital part of this.

For example, when a client is engaged in speculative derivative trades and is trading from behind the purported anonymity of an offshore trust, the regulated firm has to demonstrate a very high degree of 'due diligence' in the client's case. It is a matter of practical necessity that the institution has to monitor the trader's conduct every day, considering how quick and easy it is for such a trader to engage in high-risk activity.

The same is true of any customer whose financial affairs are fluid and subject to quick changes. It is therefore true of every retail financial institution's customer.

What most existing anti-money laundering detection solutions seek to offer is nothing more than a 'snapshot in time' of the state of play on an account every week. Sometimes the system only looks every month or even every three months; this tells an investigator virtually nothing.



## Tales of the Unexpected

"Suspicion" is not defined by the courts in most jurisdictions and therefore every reporting firm's compliance manager or MLRO must interpret it. From this first step in the risk-based approach, much else follows. The British MLRO has to contend with the possibility that their interpretation of "suspicion" will be overturned by a court ruling, but that officer still has to interpret the word. The MLRO also has room to manoeuvre elsewhere.

The MLRO is entitled, for example, to assume that all clients are law-abiding citizens and will use their accounts in a lawful manner. This assumption can continue until such time as the converse is proved. If we follow this line of reasoning, the officer is also entitled to assume that the activity observed is 'normal' for that customer's account.

That activity can therefore become the 'benchmark of normality' and can form the MLRO's idea of 'usual activity' on the account. Once the MLRO decides to do this, all they have to do is to monitor the activity every day, ideally with an automated transaction monitoring system.

The officer can now ignore almost anything that is going on within the bounds of 'normal activity' because it is 'usual' or 'expected.' This unlocks their time to focus on what is 'abnormal' or 'unexpected' or 'unusual.'

It is up to each institution to decide how much emphasis it wishes to place on a certain 'alert' level. This is another freedom of choice that the risk-based approach brings, allowing the MLRO to gauge the level of risk to their firm posed from each of their client's activities.

Once the system has targeted a transaction that has occurred outside the acceptable parameters of 'normality,' it should then be able to pinpoint the many features of the alert it has just generated. It should then be able to establish whether it is something that needs to be followed up, or whether it is capable of reasonable explanation.

The rules behind such automatic decisions are a default setting. They should be capable of identifying and providing alerts for the vast majority of potential money laundering activities. In this light, rule-driven systems are infinitely more preferable to those systems whose architecture is 'neural' or 'intelligent,' for one very important reason.

We now come to the bane of every MLRO's life: the huge quantity of so-called 'false positives' which most 'intelligent' IT systems throw up regularly.

False positives are alerts which a detection system identifies but which, upon examination, prove to be unfounded. In a fraud detection system, the institution can decide which alerts it will and will not investigate. The problem is that all money laundering alerts have to be investigated.

The minimization of 'false positives' is therefore a priority for every system. The MLRO should be able to deal with the problem by being able to calibrate the 'sensitivity' of the alert profile. The MLRO must try their best to align it as closely as possible to the risk profile that they have given to their institution.

## Detect, Inspect, Resolve

Financial practitioners have a risk-based right to assume that all their clients will manage their financial affairs in a legal, decent and truthful manner, until such time as the contrary is proven. It does not mean, however, that the financial practitioner can afford not to undertake the most careful monitoring to ensure that their initial impression is justified.

The true skill of the compliance manager will be judged from now on by their skill at maintaining a good relationship with clients while remaining alert to every nuance of client activity. When such conduct diverges from the straight and narrow, it inevitably becomes a matter for the judgement of others, and they may not be willing to share the compliance manager's opinions. One person's subjective judgement of compliance can lead to another person's allegation of negligent misconduct!

A primary requirement of an electronic system is the provision to manage clients' financial information holistically.

This is the realm of transaction monitoring: the ability to monitor and observe every single client transaction; to place it in its financial context; to compare it with historical activity; to identify the volume of transactions which are occurring inside the account at any given point in time, and to determine whether these are part of a normal range of actions, or are unusual and therefore worthy of evaluation. This is also the realm of false positive ratios which every system must keep within acceptable limits. All these requirements and more can be managed through the sort of transaction monitoring identified in this document.

A successful transaction monitoring service always requires skilled understanding coupled with good training. It requires dedicated personnel with a sound grasp of financial crime case studies and methods. When properly calibrated, installed in concert with a sound risk management policy, and driven by a skilled compliance practitioner, it can give the professional user the extra edge in compliance management. It can, in short, allow financial practitioners to 'know their customers' as well as they can.

To find out more about Complinet's transaction monitoring solution – TransWatch, please visit [www.complinet.com/transwatch](http://www.complinet.com/transwatch)



## About the author

Rowan Bosworth-Davies is widely recognized as one of the foremost teachers and consultants in the field of fraud prevention and anti-money laundering awareness.

A legal consultant and a former Fraud Squad detective at New Scotland Yard, he ran the investigations division of one of the UK's financial self-regulatory organizations for two years.

Bosworth-Davies subsequently spent ten years working for prestigious law firms in the City of London as a criminal justice consultant. He is an academic with a Visiting Fellowship at the London School of Economics, appointed a Churchill Fellow in 1995, and the holder of Honorary Research Fellowships at Exeter University and the Institute of Advanced Legal Studies, and provides regular lectures on white-collar crime issues at British universities and law enforcement training centers.

A Master of Arts of Exeter University, he has spent more than 25 years studying, investigating, prosecuting and writing about fraudsters and white-collar criminals. He is the joint author of the leading practitioner's text book, **Money Laundering - — A Practical Guide To The New Legislation**. His other works on the subject of white-collar crime include:

**Fraud in the City — Too Good To Be True** (*Bodley Head, 1986*);

**The Regulation and Prevention of Economic Crime Internationally** (*Kogan Page, 1995*); and

**The Impact Of International Money Laundering Legislation** (*Financial Times Management Reports, 1997*).

A regular contributor to *Money Laundering Bulletin* and *Fraud Intelligence*, the leading compliance publications in the UK, and the former editor of the *Financial Times Fraud Report*, he sits on the Money Laundering Editorial Board of *Complinet*, the leading compliance website.

Most recently the director of the Fraud and Anti-Money Laundering Solutions Program for SAS International, an anti-crime software provider, he now advises and trains officials and staff at government departments and leading financial institutions all over the world. He also provides governments and banks with strategic advice about financial crime prevention.