Keeping trading companies compliant

The role of management-information software in helping to tackle market abuse

Gary Bennett
VP sales UK & Ireland, Enghouse Interactive
marketingemea@enghouse.com

While precise and uniform definitions of market abuse can be hard to pin down, it is typically seen as taking two forms:

- Market manipulation – where somebody knowingly gives out false or misleading information – about a company's financial situation, for example – in order to influence the price of a share for personal gain.
- Insider dealing – where a person who has information not available to other investors – a senior member of staff with knowledge of a pending merger or acquisition, for instance – uses the information for personal profit.

An evolving regulatory environment

Financial-services organisations have a duty to take action to counter market abuse conducted by their employees, of course. It is a responsibility that is being reinforced by a string of industry regulations.

The 2010 US Dodd-Frank ruling against market manipulation, puts in place stringent reporting and record-keeping requirements. The Markets in Financial Instruments Directive (MiFiD), which has been applicable across the European Union since November 2007 and is being updated in 2018, sets out regulatory reporting to avoid market abuse.

There has also been a raft of in-country directives from bodies such as the Financial Industry Regulatory Authority, the Swiss Financial Market Supervisory Authority, as well as the UK's own Financial Conduct Authority (FCA).

In addition to regulatory changes (which not all finance organisations have fully adhered to), there have also been a raft of fines issued for non-compliance, which have been well documented in industry press.

It is estimated that one in 10 new bank employees, taken on over the past three years, have been brought into compliance teams

In July 2016, the new EU Market Abuse Regulation (MAR) came into force, placing yet greater onus on financial-services companies and individuals to detect, and act upon, suspicious activity and malpractice within their organisation.

The regulation has implications on transactions, orders and behaviours relating to any financial instruments. The penalties for non-adherence to MAR are robust and will be stringently applied.

Today, this new, even tougher, regulatory environment is forcing financial-services organisations to take action to tighten up their processes. Whereas, previously, rulings were primarily advisory and failure to comply was typically met by little more than a 'warning shot across the bows', today, regulatory bodies are increasingly insisting that this kind of capability is in place. Financial organisations are, in turn, expected to show that they have conducted due diligence and have implemented the correct governance procedures, and the best systems and processes, to enable detection of any potential breaches.

Implementing a solution

As a result of this shift in the regulatory landscape, organisations are having to change their approach to dealing with market abuse. They can no longer get by adopting procedures based on passively monitoring behaviour. Instead, they need to start embracing approaches that are founded on actively tracking it.

In the past, the focus was on recording calls and storing the information away in bulk so that it was available for the authorities to sift through painstakingly if required.

That, in itself, was a huge job for the organisations concerned, but the most recent legislation requires them to retain much more comprehensive records, including records of all transactions, whether verbal, written, or telephonic. As a result, organisations across the sector are now increasingly focused on putting in place the right tools and functionality.

They have already invested a great deal of time, effort and resource into resolving these issues. It is estimated that one in 10 new bank employees, taken on over the past three years, have been brought into compliance teams, marking a decided shift away from the historical focus around traders and front-office staff.

Unfortunately, that will not be sufficient to solve the problem. Banks and other financial-services companies will also need to ensure that they are implementing the right technological solutions.

Fortunately, products like Proteus Trader, from Enghouse Interactive, have a proven track record in this market and are increasingly forming part of the 'compliance toolkit' within institutions. One of the key

upfront challenges that compliance teams face, when protecting against suspicious transactions, market manipulation, or insider dealing, is locating a divergence from typical trends of activity. A trader could make multiple communications in any day, to a variety of different internal and external colleagues and clients.

Over time, call data can establish the average activity levels, of both duration and volume of calls, for each trader. If the average is exceeded by a certain percentage, then a report will be sent to a compliance manager to indicate the threshold breach. This could then trigger a further investigation into the data to cross-reference why activity has exceeded normal practice.

This kind of system can also be used to get a much clearer picture of trader behaviour at a more granular level, effectively establishing, for example, that trader X called number Y at a particular time on a particular day, and then called the same number five further times over the course of the same week.

In addition, solutions can be deployed to enable financial-services organisations to capture the content of calls. Generally, that will entail first recording them and then running speech analytics on them in order to identify words or phrases that might raise suspicion or be relevant to a specific search that they are already undertaking.

This kind of functionality can be very helpful to the authorities, typically including the FCA and the compliance team at the bank. It can effectively help them to quickly and proactively find a specific recording relating to what is perceived to be untoward activity on behalf of the trader.

Moving to a fully proactive approach

Some banks today are looking to go further than just actively monitoring. Instead, they want to be more proactive still by blocking calls. This could take the form of gateway blocks put in place to prevent calls to certain countries, for example, or it could involve a more specific ban on trader X contacting trader Y altogether.

The latest management-information software, such as Proteus, can potentially help with both of these scenarios. Any attempt at such calls can be blocked immediately and notifications sent directly to the compliance team – but the keynote here is flexibility. If organisations want to allow these kinds of calls to happen, and then pick them up later as compliance issues, they can do that also.

Consultancy is key

Of course, implementations of these kinds are not just about putting systems in place. There also needs to be an accompanying process of close engagement between vendor and end customer.

From the vendor's perspective, the hardest part of the equation is understanding exactly what the customer views as non-compliant or prohibited behaviour. There is a temptation to think this would be largely standard across the board. However, that is far from the case.

So, the first stage for the vendors is understanding which contacts are banned and which actively encouraged, and, from that, start configuring accurate contact lists. Once this process is completed they can start to install the systems themselves. Typically, it is a process that takes around six to eight weeks to finalise.

Some banks today are looking to go further than just actively monitoring

In conclusion

In practical terms it is extremely difficult for a financial-services organisation to guarantee that it will be able to prevent any abuse or malpractice. The responsibility, however, is now placed firmly at the door of the trading companies to implement robust systems that, primarily, aim to stop bad practice, but can, in the event of an infraction, be quick to detect and provide evidential data to enable them to report it swiftly and concisely.

The latest management-information systems are a key aspect of the compliance team's war-chest in relation to complying with MAR and, used as part of the broader structure of data management, can provide not only post-event capture but also help protect, or even deter, from potential transgression. CCR