KPMG

The Market Abuse Regulation

Changing minds and machines

June 2016

With just two weeks left on the clock till the implementation deadline for the Market Abuse Regulation (MAR), many firms have already invested considerable sums of money and energy in analysing and mapping the requirements of MAR. They have subsequently moved into implementation phases. Ahead of the deadline, we pause to consider the impact which the conceptual shifts in MAR is having on firms, the broader direction of travel in this space and why this is all causing such a stir.

Plugging into the future

The idea of plugging into machines to foresee crimes and arrest suspects before those crimes are committed were fantasties found in 1950s science fiction tales such as The Minority Report. Today, such fantasies may become a reality driven, in part, by some of the conceptual shifts and demands stemming from the Market Abuse Regulation (MAR).

The requirements of MAR will take effect on 3 July 2016. MAR is being issued by the European Securities and Markets Authority (ESMA). It is accompanied by the Directive on Criminal Sanctions for Insider Dealing and Market Manipulation (CSMAD). Though some jurisdictions, such as the UK and Denmark, have opted out of CSMAD under the Lisbon Treaty, MAR itself is directly applicable.

MAR will repeal and replace the Market Abuse Directive which underpins the existing market abuse regime. It extends that existing regime to cover new products, platforms and markets. MAR applies to any financial instrument traded on a regulated market, a Multilateral Trading Facility or an Organised Trading Facility, and it covers any conduct or action which can have an effect on such a financial instrument.

MAR is, in part, driven by technological innovation and is, in turn, a driver for technological innovation. The evolution of trading technology, the arms race for speed, the proliferation of trading venues and the increasing complexity in how trading products are structured are all factors that placed a great deal of pressure on regulators to match pace by renewing regulation. In turn, the requirements of MAR necessitate more sophisticated technological capabilities to allow firms to comply, particularly in the context of surveillance.

Conceptual shifts – complex and costly

MAR alters the current regime with some significant conceptual shifts. For example, by introducing the offence of attempted market manipulation, MAR expands the focus of the existing regime from actual damage done or market abuse committed, to penalising failed attempts and essentially punishing traceable intentions, which may have been acted upon, but ultimately did not lead to market manipulation. In legal terms, it could be argued that we are seeing a shift from focussing on 'Actus Reus' to also considering 'Mens Rea'. Responding to such conceptual shifts and the other requirements of MAR is proving a costly and complex challenge for firms.

Making it personal

The discovery of behaviour which may constitute market abuse has clear consequences for the firms whose names are splashed across the headlines. To name a few: significant fines, reputational damage, loss of clients, loss of revenue, loss of permissions to carry out specific regulated activities, drops in share price, cost of large scale remediation exercises, litigation fees.

We are now also seeing a visible drive towards individual accountability and repercussions for both individuals involved in the commission of offences, as evidenced by a series of high profile criminal prosecutions, and also, going forwards, those who are charged with meeting regulatory requirements and upholding standards in this space. Within the UK, the latter is driven further in part by the requirements of the Senior Managers and Certification Regime (SMCR). There is a possibility that the standards within SMCR may get some traction in other jurisdictions through the adoption of harmonised standards by global players.

Sink or swim

So where does MAR end and where do other pieces of regulation looming over the same firms begin? Examples include the Markets in Financial Instruments Directive II (MiFID II), the Regulation on Wholesale Energy Markets Integrity and Transparency (REMIT) and the SMCR.

Taking a holistic view of this sea of regulation and identifying points of overlap is the key to swimming rather than sinking. The importance of capitalising on these points of overlap and how to begin identifying them is discussed in KPMG's Preparing for MAR and MiFID II: Capitalising on the Synergies.

Failing to prepare is preparing to fail

How are firms preparing for MAR? Over the last 12 months, firms have been carrying out MAR mapping exercises, impact assessments and, more generally, market abuse risk assessments. They are re-drafting policies and procedures, training staff and re-designing systems and controls.

Many firms are reviewing their surveillance processes resulting in a great number of those firms investing in automated trade surveillance solutions or enhancing their existing solutions. To compliment these investments in surveillance technology, some banks are bringing in senior figures from intelligence agencies, like MI5, who were previously conducting surveillance on violent criminals and terrorists.

A number of firms are taking a more holistic approach to surveillance and are building more sophisticated audio communications and electronic communications monitoring technology into their surveillance programmes.

Technology is the answer…but what is the real question?

Effective technology solutions with more sophisticated capabilities and the ability to handle greater data streams are the key to meeting some of the more challenging requirements in MAR. The rationale for this becomes clear when considering requirements, such as not only reporting suspicious transactions but also reporting suspicious orders as part of the new STORs regime and being able to detect attempted market manipulation as well as actual market manipulation.

Some firms, particularly banks on Wall Street, are taking this one step further and are starting to use artificial intelligence-based technology developed by companies backed by the CIA. They are monitoring different types of behaviour exhibited by their employees and performing data-driven behavioural analysis in order to identify patterns, with the eventual aim of predicting who is likely to commit a crime. An understanding of behavioural economics, behavioural finance or human psychology could also supplement this technology and present a distinct advantage in the fight to predict, prevent and deter rather than just detect post-act.

Mouse cursor tracking, computer screens with retina tracking technology, wristbands which can detect heart rates and track body temperature - there is a great deal of technology available for those who are trying to play the Minority Report game.

Firms will need to consider their duty to meet demanding regulatory requirements in this space and their need to avoid the many layers of costs which engulf them when market abuse activity occurs and is uncovered. They will need to balance this with respecting and proventing the privacy and freedom of their employees. Each firm will need to ask itself how much weight to apportion these competing priorities and how far to take their market abuse prevention strategies - the technology is out there.

Contact

Rabya Anwar

Principal Regulatory Advisor
+44 (0)7785 660 723
rabya.anwar@kpmg.co.uk

kpmg.com/uk/futurefs

CREATE | CRT063697 | June 2016