RBC Investor & Treasury Services

Meeting global financial market challenges

Financial services organisations are required to comply with an increasing range of regulatory compliance initiatives designed to provide greater resiliency in response to unexpected shocks, and increased investor transparency.

Against this backdrop, market participants are also facing other rapidly evolving themes and scenarios such as:

- the United Kingdom's (UK) referendum vote to leave the European Union (Brexit)
- the growing spectre of cyber security threats
- the emergence of digital currencies and blockchain

Tony Freeman, Executive Director of Industry Relations at the Depository Trust and Clearing Corporation (DTCC), recently addressed these pressing topics at an exclusive forum hosted by RBC Investor & Treasury Services.

Drawing on insights gained from DTCC's expertise as a global post-trade infrastructure provider, which processes trillions of dollars of securities transactions daily, Freeman suggested that every financial services business must remain vigilant around regulatory issues and emerging cyber threats.

Evolution of derivatives

The second Markets in Financial Instruments Directive (MiFID II) is a significant regulatory initiative that aims to create a single market for investment services and ensure a high degree of harmonised protection for investors.

The MiFID II framework governs European Union-based firms that provide services to clients who trade financial instruments, including equities, bonds and derivatives. The rules encompass front office trading and herald some of the most significant shifts in the way financial instruments will be exchanged in the EU.

Following the UK referendum result, London has become a focus for market participants given its current status as the leading European derivatives market. Based on current circumstances, the UK will be initially required to comply with the MiFID II directive, however, soon after the rules come into force, it is possible that the UK may no longer be part of the EU. How London might address this situation remains unknown. Whatever the terms of its withdrawal, UK regulators will need to appropriately engage with the European derivatives markets within the bloc.

There are precedents where regulators from different jurisdictions, such as Australia and Singapore, have recognised each other's governance framework as 'equivalent', effectively making them interchangeable. This may be a potential way forward for derivatives regulation between the UK and the EU.

> *"MiFID II is a significant piece of legislation that will change the business model for many financial market participants"*

MiFID II is a significant piece of legislation that will change the business model for many financial market participants, and forms part of a broader global push towards the 'electronification' of financial markets.

The rules stem from a political desire to make over-the-counter markets more transparent and apply equity market practices to derivatives and other markets, such as the requirement for instruments to be traded on a public exchange.

The effect of MiFID II may mean that instead of transacting relatively large trades in the in-scope financial instruments, trading will be more frequent but in smaller sizes. This was also the result when rules relating to trading in foreign exchange products were tightened. Organisations that trade financial instruments must consider how they will adapt their business model to this revised regime.

A related legislative initiative in the US is the Legal Entity Identifier (LEI) project mandated by the European Securities and Markets Authority (ESMA), which was initiated in response to the 'flash crash' that impacted markets during May 2010.

The LEI initiative effectively adds a bar code to financial market participants so they can be more easily identified. Australia has agreed to the LEI rules and any business trading US equities is required to have an LEI. Tony encouraged institutions to ensure they have an LEI strategy in development alongside a clear implementation strategy.

Blockchain potential

Financial services businesses and markets regulators are also exploring the potential for distributed ledger technologies, such as blockchain, to make the operation of financial markets more efficient.

Substantial research is being undertaken globally to gauge blockchain's full potential and a number of financial services firms are exploring ways in which they might harness this emerging technology. For example, the Australian Securities Exchange (ASX) is currently engaged in a project to explore the potential for blockchain to add back office and settlement efficiencies to its platform.

While Tony thought it unrealistic to assume that blockchain would replace trading platforms or dislodge central clearing house functionality, he did believe there is potential for its application among other instruments such as credit default swaps. He cautioned market participants to expect the pace of change to be rapid and encouraged them to grasp blockchain's potential as soon as possible.

Brexit and financial markets

The terms of the UK's withdrawal from the European Union are as yet unknown, but the British government has stated its intention to leave the bloc by March 2019.

There was some discussion prior to the referendum projecting that investment banks might leave Britain in the event of Brexit. Tony concluded this was an unlikely scenario given that few jurisdictions would have financial market infrastructure to supervise banks that re-domicile from Britain. While Frankfurt and Dublin have been suggested as viable alternatives, their financial market ecosystems and community resources do not have the necessary scale to support such a move.

> *"Market participants should expect the pace of change to be rapid"*

Spotlight on cyber security

Cyber security is a persistent concern in financial markets, and interest became further heightened after hackers compromised the SWIFT system in June 2016.

Currently, global co-ordination on cyber security in financial markets is fragmented, with multiple regulations applicable across many jurisdictions. In markets such as the US, principled-based and rules-based regimes apply concurrently. This arrangement has produced a complex regulatory environment in relation to cyber security.

An interesting development may be independent verification of financial institutions' cyber security practices in order that businesses can prove to regulators they have appropriate security practices in place. Public disclosure of security practices is not always feasible because of the risk that this information could, in itself, result in breaches. Third-party verification may be the most secure way to provide regulators sufficient comfort that the businesses they oversee are effectively mitigating their cyber security risks.

Overall, the global regulatory landscape remains exceptionally active. The onus is on financial market participants to remain cognisant of emerging regulations and ensure their strategic approach is sufficiently robust to meet their obligations.